Universidade Estadual de Campinas
Instituto de Matemática Estatística e Computação Científica
Departamento de Matemática

Sobre a Existência de Elemento Primitivo Para Extensões Separáveis de Anéis Comutativos

Dirceu Bagio[†]
Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Antonio Paques

[†]Este trabalho teve apoio financeiro do CNPQ.

Sobre a Existência de Elemento Primitivo Para Extensões Separáveis de Anéis Comutativos

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Dirceu Bagio** e aprovada pela comissão julgadora.

Campinas, 26 de janeiro de 2004.

_____

Prof. Dr. **Antonio Paques**.
Orientador

Banca examinadora:

Prof. Dr. Antonio Paques (Orientador, IMECC - UNICAMP)
Prof. Dr. Franscisco César Polcino Milies (IME - USP)
Prof. Dr. Hector A. Merklen Goldschmidt (IME - USP)
Prof. Dr. Miguel Angel Alberto Ferrero (IM - UFRGS)
Prof. Dr. Paulo Roberto Brumatti (IMECC - UNICAMP)

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do título de **Doutor em Matemática**.

Aos meus pais

Agradecimentos

Agradeço:

• a minha família, pelo incentivo concedido em todos os momentos.

• aos colegas de pós-graduação Adélia, Amauri, Daniel, Daniela, Edson, Ercílio, Fábio, Flávia, Geovani, Ilma, Irene, Juliana, João, Jones, Luciana, Luciano, Marcela, Marina, Marcos, Paulo, Paulo César, Roger, Ronan e Yurilev, pela agradável companhia.

• aos amigos Ari, Danilo, Juliano, Paula, Rogério, Romário e Weber, com os quais tive a satisfação de formar "república".

• ao Curso de Pós-Graduação em Matemática do IMECC pela acolhida e aos professores que direta ou indiretamente contribuiram na minha formação.

• aos funcionários da secretaria de pós-graduação Cidinha, Edinaldo e Tânia, por suas esclarecedoras explicações.

• ao CNPQ (Conselho Nacional de Desenvolvimento Científico e Técnológico), pelo auxílio financeiro recebido.

A minha namorada Elisabeth, minha gratidão pelo seu companheirismo e pela sua paciência nos momentos de dificuldade e de ausência.

Meus sinceros agradecimentos ao meu orientador Antonio Paques, tanto pela atenciosa e competente orientação, quanto pela amizade.

Resumo

Um dos teoremas clássicos da teoria de Galois para corpos é o teorema do elemento primitivo. Na teoria de Galois para anéis comutativos com unidade, tal teorema não é válido em geral. Nesse trabalho encontramos condições necessárias e suficientes para a existência de elemento primitivo para uma extensão fortemente separável de um anel comutativo com unidade e cujos únicos idempotentes são os triviais. Além disso, apresentamos uma forma fraca deste teorema e provamos que esta forma fraca é válida para anéis conexos cujo quociente pelo radical de Jacobson é von Neumann regular e localmente uniforme. Analisamos também o fecho separável de um anel comutativo conexo. Obtemos alguns resultados que relacionam, em particular, o fecho separável do anel com o fecho separável de cada um de seus corpos residuais.

Abstract

One of the classic theorems of the Galois theory of fields is the "Primitive Element Theorem". In Galois theory of commutative rings, such a theorem does not hold, in general. In this work we give necessary and sufficient conditions for the existence of a primitive element in an strongly separable extension of a connected commutative ring. Furthermore we present a weak form of the Primitive Element Theorem and we prove that this theorem holds for strongly separable extensions of connected commutative rings whose quotient by its Jacobson radical is a von Neumann regular and locally uniform ring. We also obtain some new results about the separable closure of a connected commutative ring. In particular, we describe a relation between the separable closure of such a ring and the separable closure of each one of its residual fields.

Sumário

Introdução

Um dos teoremas clássicos da teoria de Galois para corpos é o teorema do elemento primitivo. Ele nos diz que, dada uma extensão separável e finita de corpos K/F existe $\alpha \in K$ tal que $K = F[\alpha] = \{f(\alpha) \ : \ f(X) \in F[X]\}$. Lembremos que cada extensão galoisiana de corpos é separável. Portanto, toda extensão galoisiana finita de corpos tem elemento primitivo.

Em 1960, M. Auslander e O. Goldman definiram em [2] o conceito de extensão galoisiana de anéis comutativos com unidade. Em seguida, S. Chase, D. K. Harrison e A. Rosenberg em [3], não somente encontram condições equivalentes a definição dada em [2], mas também desenvolvem a teoria de Galois para anéis comutativos com unidade. Entre outras coisas, provaram um teorema análogo ao teorema fundamental, encontrando uma bijeção entre os subgrupos do grupo de Galois e "certas" subálgebras intermediárias.

A pergunta natural que se faz é a seguinte: o teorema do elemento primitivo continua válido no contexto de anéis comutativos com unidade? Ou seja, dada uma extensão galoisiana S/R de anéis comutativos existe $\alpha \in S$ tal que $S = R[\alpha] = \{f(\alpha) \ : \ f(X) \in R[X]\}$? Em geral, a resposta para esta pergunta é não. Existem vários exemplos de extensões galoisianas que não possuem elemento primitivo. Dentre tais, veremos no decorrer do trabalho que $S = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z}$ não possui elemento primitivo.

Muitos trabalhos relacionados com a existência do elemento primitivo aparecem na literatura. O Lema 3.1 de [14], diz que se $(R, \mathcal{M})$ é um anel local tal que $\left|\frac{R}{\mathcal{M}}\right| = \infty$ então cada extensão separável e finitamente gerada (como módulo) tem elemento primitivo. Este resultado foi melhorado e estendido para anéis semilocais em [27]. J-D. Thérond prova que se R é um anel semilocal e $Max(R) = \{\mathcal{M}_1, \ldots, \mathcal{M}_t\}$ então cada extensão separável de posto n tem elemento primitivo se e somente se $\left|\frac{R}{\mathcal{M}_i}\right| \geq n$ para todo $1 \leq i \leq t$. Em seguida, o resultado de J-D. Thérond foi generalizado por A. Paques. O Teorema 2.4 de [26], afirma que cada extensão separável de um LG-anel R de posto n tem elemento primitivo se e somente se $\left|\frac{R}{\mathcal{M}}\right| \geq n$, para todo

$\mathcal{M} \in Max(R)$. Note que o conjunto de LG-anéis inclue anéis semilocais e anéis os quais são von Neumannn regular módulo o seu radical de Jacobson.

Destacamos também os trabalhos de I. Kikumasa, T. Nagahara e K. Kishimoto. Em [17] e [15], faz-se um estudo amplo sobre a existência do elemento primitivo para uma extensão galoisiana de um anel semilocal. Dentre outras coisas, prova-se que se R é um anel comutativo com unidade e semilocal e $Max(R) = \{\mathcal{M}_1, \ldots, \mathcal{M}_t\}$ então uma extensão galoisiana S/R tem elemento primitivo se e somente se $\frac{S}{\mathcal{M}_i S}/\frac{R}{\mathcal{M}_i}$ tem elemento primitivo para cada $i \in \{1, \ldots, t\}$. No Teorema 5 de [16], I. Kikumasa e T. Nagahara encontram condições para que uma extensão cíclica de grau 2^2 possua elemento primitivo. Este resultado foi generalizado por A. Aramova em [1], para extensões cíclicas de grau p^n, onde p é um número primo positivo.

Em todos os trabalhos citados acima, estuda-se o problema da existência de elemento primitivo para uma extensão S/R fazendo-se alguma restrição sobre o anel R. O propósito do nosso trabalho é fazer um estudo geral deste problema, no seguinte sentido: consideramos uma extensão galoisiana (ou, separável, projetiva e finitamente gerada) S/R, onde R é um anel comutativo com unidade arbitrário. Podemos então, via o Teorema 2.1.2 da seção 2.1, reduzir nosso estudo ao caso em que R é conexo. De fato, tal teorema afirma que S/R tem elemento primitivo se e somente se S_x/R_x tem elemento primitivo para cada $x \in X(R)$, onde $X(R)$ denota o espectro booleano do anel R (ver Definição 1.2.1). É sabido que R_x é um anel conexo para todo $x \in X(R)$ (veja Teorema 1.2.12).

No que segue, descreveremos os principais resultados obtidos neste trabalho. No capítulo 2, consideramos uma extensão fortemente separável S/R (isto é, S é uma R-álgebra separável e um R-módulo projetivo e finitamente gerado) com R conexo. Assuma que $S = S_1 \oplus \ldots \oplus S_r$ é a decomposição de S em componentes conexas. Provamos que S/R tem elemento primitivo se e somente se existem $f_1, \ldots, f_r \in R[X]$ tais que $\frac{R[X]}{(f_i)} \simeq S_i$ e $(f_i) + (f_j) = R[X]$ para $i \neq j$. Observe que não é suficiente exigir que cada componente conexa possua elemento primitivo para que S/R tenha elemento primitivo, como mostra o exemplo $S = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z}$. De qualquer forma, as componentes conexas possuirem elemento primitivo é uma condição necessária para que S/R possua.

No terceiro capítulo exploramos a construção dos polinômios $f_i's$ necessários para a existência do elemento primitivo. Assumindo que uma das componentes conexas possui elemento primitivo, construimos sob certas condições, polinômios que geram a mesma extensão e que são fatores irredutíveis de um polinômio separável. Então,

pelo Lema 1.2 de [11], tais polinômios são comaximais. Obtemos assim condições suficientes para que uma extensão fortemente separável possua elemento primitivo. Os resultados obtidos neste capítulo generalizam os resultados de [6], pois C. Dragos trabalha no contexto de corpos. Além disso, utilizamos uma visão categórica dada em [11] para decidir quando dois polinômios geram a mesma extensão e quando um polinômio é normal, seguindo as definições dadas em [6].

Observe que para a construção dos polinômios $f_i's$ exige-se que a componente conexa possua elemento primitivo. No entanto, existem extensões fortemente separáveis e conexas que não possuem elemento primitivo (ver exemplo da seção 2.4). Mais do que isso, existem extensões fortemente separáveis e conexas de um anel local que não possuem elemento primitivo (ver [32, pg.170]). Em [23], T. McKenzie apresenta uma forma fraca do teorema do elemento primitivo para anéis locais: dada uma extensão S/R fortemente separável e conexa com R um anel local, é possível mergulhá-la numa extensão fortemente separável e conexa T/R com $T = R[\alpha]$. No capítulo 4, estendemos o resultado acima obtendo a forma fraca do teorema do elemento primitivo para uma extensão de uma anel conexo R tal que $\frac{R}{J(R)}$ é von Neumann regular e localmente uniforme.

No primeiro capítulo, introduzimos algumas definições básicas e exploramos as principais propriedades do espectro booleano de um anel. Além disso, seguimos a construção feita por A. Magid em [19], para provar a existência do fecho separável Ω_R para um anel conexo R.

No último capítulo, aplicamos os resultados obtidos nos capítulos anteriores para generalizar alguns resultados de T. Mckenzie. O Lema 4.8 de [21], afirma que se $(\Omega_R, \mathcal{M}')$ é local então $\Omega_{\left(\frac{R}{\mathcal{M}}\right)} = \frac{\Omega_R}{\mathcal{M}'}$, onde $\mathcal{M}' \cap R = \mathcal{M}$. Provamos que se R é um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular então $\Omega_{\left(\frac{R}{\mathcal{M}}\right)} \simeq \frac{\Omega_R}{\mathcal{M}'}$, onde $\mathcal{M}' \cap R = \mathcal{M}$. Também em [21] prova-se que se $(\Omega_R, \mathcal{M}')$ é local e $I \subseteq R$ é um ideal então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$. Estendemos este resultado da seguinte forma: se R é um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $I \subseteq R$ é um ideal tal que $\frac{\Omega_R}{I\Omega_R}$ é conexo então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$. Em [22], define-se quando um anel local $(R, \mathcal{M})$ é fracamente henseliano da seguinte maneira: se cada polinômio separável e irredutível em $R[X]$ permanece irredutível em $\frac{R}{\mathcal{M}}[X]$ dizemos que R é um anel fracamente henseliano. O Teorema 1.5 de [22] afirma que R é fracamente henzeliano se e somente se Ω_R é local. Os resultados da seção 5.1 estendem este teorema.

Fixemos agora algumas notações e convenções. Em todo este trabalho, salvo menção em contrário, todos os anéis são comutativos com unidade e homomorfismos

de anéis levam unidade em unidade. Denotamos por $U(R)$ o grupo multiplicativo formado pelos elementos invertíveis de R. Uma extensão S/R é dita projetiva (finitamente gerada) se S é um R-módulo projetivo (finitamente gerado). Um anel R é dito conexo se $Spec(R)$, com a topologia de Zariski, é um espaço topológico conexo. Note que R é conexo se e somente se os seus únicos idempotentes são 0 e 1. Em particular, anéis locais e domínios são exemplos de anéis conexos. Para um anel R, denotaremos por $J(R)$ ($N(R)$) o radical de Jacobson de R (o nilradical de R) , ou seja $J(R)$ é a intersecção de todos os ideais maximais de R (ou seja, $N(R)$ é a intersecção de todos os ideais primos de R). Dado um polinômio $f(X) \in R[X]$ indicaremos o seu grau por ∂f ou $\partial(f)$. Seguindo [25], denotaremos por $\delta(f)$ o discriminante de um polinômio mônico $f \in R[X]$. Se G é um grupo e H é um subgrupo de G denotaremos por $[G : H]$ o índice de H em G.

Capítulo 1

Pré-Requisitos

Na primeira seção desse capítulo introduzimos as definições que serão utilizadas com maior freqüência nesse trabalho. Apesar de tais definições serem clássicas, as reproduzimos aqui para a comodidade do leitor. Na segunda seção abordamos conceitos e resultados relacionados com álgebras booleanas. Estes conceitos e resultados aparecem na literatura, mas não são tão comuns. Estudamos o espectro booleano $X(R)$ de um anel comutativo R e a sua topologia. Finalizamos o capítulo, seguindo a construção feita em [19] para provar a existência do fecho separável de um anel comutativo conexo.

1.1 Definições Básicas

Apresentamos nessa seção, os três principais conceitos utilizados nesse trabalho: álgebra separável, polinômio separável e extensão galoisiana. Iniciamos com a definição de álgebra separável.

Sejam R um anel e S uma R-álgebra (não necessariamente comutativa). Considere a álgebra envolvente $S^e = S \otimes_R S^o$, onde S^o é a álgebra oposta. Observe que S é um S^e-módulo à esquerda com a operação definida por: $(a \otimes b).c = acb$.

Lema 1.1.1. *[5, Proposição II.1.1] As seguintes afirmações são equivalentes:*

i. S é um S^e-módulo à esquerda projetivo.

ii. A sequência exata de S^e-módulos à esquerda $0 \longrightarrow J \longrightarrow S^e \xrightarrow{\mu} S \longrightarrow 0$ cinde , onde μ é a função multiplicação e $J = Ker(\mu)$.

iii. Existe $e \in S^e$ tal que $\mu(e) = 1$ e $Je = 0$.

Definição 1.1.2. *Uma R-álgebra S satisfazendo uma das condições equivalentes do lema acima é dita separável.*

Outras caracterizações e resultados sobre álgebras separáveis podem ser vistos em [2], no capítulo 2 de [5] e em [14].

Consideramos agora a definição de polinômio separável.

Definição 1.1.3. *Sejam R um anel comutativo e $f(X) \in R[X]$ um polinômio mônico. Dizemos que f é um polinômio separável sobre R se a R-álgebra $\frac{R[X]}{(f)}$ é separável.*

Note que, por definição, um polinômio separável é mônico. Apesar da redundância, muitas vezes escreveremos: seja $f(X)$ um polinômio mônico e separável.

Usaremos a seção 3.4 de [5] e [14], como referências para as propriedades e resultados relacionados com polinômios separáveis.

O anel S será chamado uma extensão de R (ou S/R extensão de anéis) se S é uma R-álgebra fiel. Neste caso, note que o homomorfismo $i : R \longrightarrow S$ dado por $i(r) = r.1$ é injetivo. De fato, $Ker(i)$ é igual ao anulador de S em R. Portanto, $Ker(i) = 0$. Desta forma, podemos identificar R com $R.1 \subseteq S$.

Agora consideraremos a definição de extensão galoisiana de anéis comutativos, a qual será usada freqüentemente neste trabalho. Essa definição apareceu pela primeira vez na literatura em [2]. No entanto, tal conceito foi explorado mais amplamente em [3]. O Teorema 1.3 de [3], apresenta caracterizações equivalentes a definição de extensão galoisiana dada aqui.

Definição 1.1.4. *Sejam S/R uma extensão de anéis comutativos (isto é, S é uma R-álgebra fiel), e G um subgrupo finito do grupo de R-automorfismos de S. Se $S^G = \{a \in S \ : \ \sigma(a) = a, \ \sigma \in G\} = R$ e existem $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma} = \begin{cases} 1, & \text{se } \sigma = 1 \\ 0, & \text{se } \sigma \neq 1 \end{cases}$ então S/R é dita uma extensão galoisiana com grupo G. Os elementos x_i, y_i $(1 \leq i \leq n)$ são chamadas as coordenadas de Galois de S sobre R.*

É uma conseqüência natural dessa definição que toda extensão galoisiana S de um anel comutativo R, com grupo G, é um R-módulo projetivo, finitamente gerado e de posto constante igual a ordem de G.

Essa definição estende o conceito de extensão galoisiana para corpos. Como é sabido se S e R são corpos é suficiente a afirmação $S^G = R$ para termos S como uma

extensão galoisiana de R. Neste caso, G é o grupo de todos os R-automorfismos de S. Mais ainda, usando o lema de Dedekind, mostra-se que a existência dos elementos x_i, y_i $(1 \leq i \leq n)$ tais que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$, para todo $\sigma \in G$ se verifica sempre (ver [31]).

1.2 Espectro Booleano

O conceito de espectro booleano é abordado com detalhes em [19]. Seguiremos este como referência para essa seção.

Seja R um anel comutativo. Considere $B(R) := \{x \in R : x^2 = x\}$, ou seja, $B(R)$ é o conjunto dos idempotentes de R. Se $+, \cdot$ são as operações de R, defina uma adição $\oplus$ em $B(R)$ por : $x \oplus y = x + y - x.y$, para todo $x, y \in B(R)$. Usando a multiplicação induzida de R, podemos verificar que $(B(R), \oplus, .)$ é um anel comutativo com unidade. Tal anel é denominado o anel booleano de R. Note que R é um anel conexo quando $B(R) = \{0, 1\}$.

De maneira usual, $Spec(R)$ denotará o conjunto dos ideais primos de R e $V(I) = \{P \in Spec(R) : I \subseteq P\}$, com I subconjunto qualquer de R serão os fechados de $Spec(R)$ segundo a topologia de Zariski. Denotamos por $X(R)$ o conjunto das componentes conexas do espaço topológico $Spec(R)$. Observe que temos uma sobrejeção natural $Spec(R) \to X(R)$, que associa a cada ideal primo a componente conexa ao qual ele pertence.

Definição 1.2.1. *O conjunto $X(R)$ munido da topologia fraca tal que a função $Spec(R) \to X(R)$ é contínua é denominado o espectro booleano de R.*

Proposição 1.2.2. *Dois ideais primos P e Q de R estão na mesma componente conexa se e somente se eles contém os mesmos idempotentes de R.*

Demonstração: É bem conhecido que a topologia de Zariski de $Spec(R)$ tem uma base de conjuntos "clopen"(aberto-fechado) $V(Re)$, com $e \in B(R)$. Seja e um idempotente de R tal que $e \in P$ e $e \notin Q$. Então, $V(Re)$ é "clopen", contém P e não contém Q. Logo, P e Q estão em componentes conexas distintas. Reciprocamente, suponha que P e Q possuem os mesmos idempotentes. Seja I o ideal de R gerado por tais idempotentes. Assim, $P, Q \in V(I)$. Mais ainda, $V(I)$ é a imagem da função contínua $Spec\left(\frac{R}{I}\right) \to Spec(R)$ induzida pela projeção $R \to \frac{R}{I}$. Procedendo como no

Teorema 1.2.12 que veremos a seguir, prova-se que $\frac{R}{I}$ é conexo. Como $V(I)$ é a imagem por uma função contínua de um espaço conexo, segue que $V(I)$ é um conjunto conexo. Conseqüentemente, P e Q pertencem a mesma componente conexa. ■

Pela Proposição 1.2.2 e pela Proposição 1.2.11 abaixo, podemos considerar uma função do espaço topológico $X(R)$ no espaço topológico $Spec(B(R))$, que para cada componente conexa de $Spec(R)$ associa o conjunto de idempotentes de qualquer elemento de tal componente. A próxima proposição justifica chamarmos $X(R)$ de espectro booleano de R.

Proposição 1.2.3. *[19, Proposição II.9] A função que associa a cada componente conexa de $Spec(R)$ o conjunto dos idempotentes de qualquer elemento de tal componente é um homeomorfismo entre os espaços topológicos $X(R)$ e $Spec(B(R))$.*

Corolário 1.2.4. *[19, Corolário II.4] $X(R)$ é um espaço topológico de Hausdorff, compacto e totalmente desconexo.*

Agora vamos introduzir uma base de conjuntos "clopen"para a topologia de $X(R)$. Verifica-se que os conjuntos "clopen"na topologia de Zariski são os conjuntos $V(e)$, com $e \in B(R)$.

Dado um idempotente $e \in R$, consideremos

$$N(e) = \{x \in X(R) \,:\, x \subseteq V(R(1-e))\}.$$

Proposição 1.2.5. *[19, Proposição II.11] Os conjuntos $N(e)$, com $e \in B(R)$, formam uma base de conjuntos "clopen"para a topologia de $X(R)$. Mais ainda, cada conjunto "clopen"de $X(R)$ é da forma $N(e)$, para algum idempotente $e \in R$.*

A próxima proposição lista as propriedades dos conjuntos $N(e)$, com $e \in B(R)$. Sua demonstração é conseqüência imediata da definição.

Proposição 1.2.6. *Sejam $e, f \in B(R)$.*

i. $N(e) \cap N(f) = N(ef)$.

ii. $N(e) \cup N(f) = N(e + f - ef) = N(e \oplus f)$.

iii. $N(e)^c = N(1 - e)$.

iv. $N(0) = \emptyset$.

v. $N(1) = X(R)$.

Dado $x \in X(R)$ considere $I(x)$ o ideal gerado pelos idempotentes de R que estão em P, para algum $P \in x$. Pela Proposição 1.2.2, $I(x)$ não depende da escolha de P. Denotamos por R_x o anel $\frac{R}{I(x)}$. O anel R_x também pode ser visto como a localização de R segundo o sistema multiplicativo $S = \{1 - e : \ e \in x\}$ (ver (2.6) de [30]). Dado um R-módulo M, denotamos por M_x o R_x-módulo $M \otimes R_x \simeq \frac{M}{I(x)M}$. Note que temos uma sobrejeção canônica natural $M \to M_x$ que associa a cada $m \in M$ a sua classe, que denotaremos por m_x.

Lema 1.2.7. *Seja M um R-módulo e $I \subseteq R$ um ideal gerado por idempotentes de R. Então, $a \in M$ está em IM se e somente se $a = ea$, para algum idempotente $e \in I$.*

Demonstração: Seja $a \in M$ e suponha que $a = ea$ para algum idempotente $e \in I$. Então $a \in IM$. Reciprocamente, seja $a \in M$ tal que $a \in IM$. Daí, $a = e_1a_1 + e_2a_2 + \ldots + e_ra_r, \ e_i \in I, \ a_i \in M$, para todo $1 \leq i \leq r$. Tome $e = e_1 \oplus e_2 \oplus \ldots \oplus e_r$ e note que $ee_i = e_i$, para todo $1 \leq i \leq r$. Logo, $ea = a$. ■

Proposição 1.2.8. *Sejam M um R-módulo, $x \in X(R)$ e $a, b \in M$ tal que $a_x = b_x$. Então existe uma vizinhança $N(e)$ de x tal que $a_y = b_y$ em M_y para cada $y \in N(e)$. Mais ainda, $e_x = 1_x$ e $ae = be$.*

Demonstração: Se $a_x = b_x$ então $a - b \in I(x)M$. Pelo Lema 1.2.7, existe um idempotente $f \in I(x)$ tal que $a - b = f(a - b)$. Tome $e = 1 - f \in B(R)$. Note que f pertence a cada um dos ideais primos que estão em x. Assim, $x \in N(e) = \{y \in X(R) \ : \ y \subseteq V(R(1 - e)) = V(Rf)\}$. Se $y \in N(e)$ então $f \in I(y)$. Logo, $(a - b) = (a - b)f \in I(y)M$. Portanto, $a_y = b_y$. Observe que $e_x = 1_x$ e $ae = be$. ■

Utilizando os resultados anteriores, provaremos que para cada $x \in X(R)$, R_x é uma R-álgebra conexa. Para tanto, ainda precisamos de alguns resultados auxiliares.

Lema 1.2.9. *Sejam S uma R-álgebra, $x \in X(R)$ e e_0 um idempotente de S_x. Então existe um idempotente $e \in S$ tal que $e_x = e_0$.*

Demonstração: Tome $f \in S$ tal que $f_x = e_0$. Observe que $f_x^2 = f_x$. Então, pela Proposição 1.2.8, existe $e_1 \in R$ um idempotente tal que $f^2e_1 = fe_1$ e $(e_1)_x = 1_x$. Tome $e = fe_1$ e note que $e^2 = e$, $e_x = f_x = e_0$. ■

Definição 1.2.10. *Sejam R um anel e $E \subset B(R)$. Dizemos que E é um ideal booleano maximal se:*

i. para cada idempotente $e \in R$ temos que $e \in E$ ou $1 - e \in E$, mas não ambos;

ii. se e e f são idempotentes de R então $ef \in E$ se e somente se $e \in E$ ou $f \in E$.

Proposição 1.2.11. *Um conjunto E de idempotentes de R é um conjunto de idempotentes de algum ideal primo de R se e somente se E é um ideal booleano maximal.*

Demonstração: Seja P um ideal primo de R e E o conjunto de todos os seus idempotentes. Se $e \in R$ é um idempotente então $e(1-e) = 0 \in P$. Assim, $e \in P$ ou $1 - e \in P$. Logo, $e \in E$ ou $1 - e \in E$. Se $e \in E$ e $1 - e \in E$ então $1 \in E \subset P$. Mas isso é uma contradição. Portanto, E satisfaz (i) da definição acima. Sejam e e f idempotentes de R tais que $ef \in E \subset P$. Desta forma, $e \in P$ ou $f \in P$. Sendo ef um idempotente, temos que $ef \in E$ se e somente se $e \in E$ ou $f \in E$. Logo, E é um ideal booleano maximal. Reciprocamente, suponha que E é um ideal booleano maximal. Assuma por absurdo que $RE = R$. Então, $1 = r_1e_1 + \ldots + r_ke_k$ com $r_i \in R$ e $e_i \in E$. Para cada $1 \leq i \leq k$, seja $f_i = e_i(1-e_1)(1-e_2)\ldots(1-e_{i-1})$. Note que o ideal gerado pelos $f_i's$ também é R. Assim, existem $s_1, \ldots, s_k \in R$ tal que $1 = s_1f_1 + \ldots + s_kf_k$. Além disso, cada f_i está em E e $f_if_j = 0$ se $i \neq j$. Multiplicando a equação acima por f_i, obtemos $f_i = s_if_i$. Conseqüentemente, $1 = f_1 + \ldots + f_k$. Desta forma, $0 = (1-f_1)(1-f_2)\ldots(1-f_k)$. Mas, $0 \in E$ e $1 - f_i \notin E$. Isso contradiz a parte (ii) da Definição 1.2.10. Logo, $RE \subsetneq R$. Tome um ideal maximal m de R tal que $RE \subseteq m$. Seja e um idempotente de m. Como $1 - e \notin m$, temos que $1 - e \notin E$. Por outro lado, $e(1-e) = 0 \in E$. Daí, $e \in E$. Isso mostra que E é o conjunto dos idempotentes de m. ■

Teorema 1.2.12. *Seja $x \in X(R)$. Então R_x é um anel conexo.*

Demonstração: Seja $e_0 \in R_x$ um idempotente. Pelo Lema 1.2.9, existe $e \in R$ um idempotente tal que $e_x = e_0$. Observe também que se $P \in x$ então $e(1-e) = 0 \in P$. Logo, $e(1-e) \in I(x)$. Pela Proposição 1.2.11, $e \in I(x)$ ou $(1-e) \in I(x)$. Portanto, $e_x = 0$ ou $e_x = 1_x$. Assim, R_x é conexo. ■

1.3 Existência e Unicidade do Fecho Separável

Da teoria de Galois para corpos, sabemos que a todo corpo K pode-se associar um corpo K_{sep} denominado de fecho separável de K. Na verdade K_{sep} é o corpo constituído de todos os elementos de algum fecho algébrico de K que são separáveis sobre K. De forma análoga, para um anel conexo R podemos construir um fecho

separável. A demonstração da existência e unicidade do fecho separável, a menos de isomorfismo, foi feita por D. K. Harrison e pode ser vista em [14].

Seguindo [14, 19], provaremos a existência e unicidade do fecho separável. Todos os resultados abordados nesta seção já apareceram na literatura. No entanto, as demonstrações dadas aqui são mais detalhadas. O leitor familiarizado com tais conceitos e resultados pode omitir esta seção.

As próximas definições são necessárias para introduzir o conceito de fecho separável e serão utilizadas com freqüência no restante deste trabalho.

Definição 1.3.1. *Sejam R um anel comutativo e S uma extensão de R (isto é, S é uma R-álgebra fiel). Dizemos que S é uma extensão fortemente separável de R se S é separável como R-álgebra e finitamente gerado e projetivo como R-módulo. Se para cada subconjunto finito $N \subseteq S$ existe uma R-subálgebra L de S a qual é uma extensão fortemente separável de R com $N \subseteq L$, dizemos que S é uma extensão localmente fortemente separável.*

Definição 1.3.2. *Quando R é conexo e a única extensão fortemente separável e conexa de R é o próprio R, diz-se que R é separavelmente fechado.*

Encontraremos a seguir uma caracterização de anel separavelmente fechado. Para tanto, precisaremos de dois resultados os quais serão apresentados sem demonstração.

Lema 1.3.3. *[29, Proposição 1.3] Se R é um anel conexo e S/R é uma extensão fortemente separável então S é uma soma direta finita de R-subálgebras conexas.*

Proposição 1.3.4. *[5, Proposição II.1.11] Se S é uma R-álgebra separável e $J \subseteq S$ é um ideal então $\frac{S}{J}$ é uma R-álgebra separável.*

Lema 1.3.5. *Um anel conexo R é separavelmente fechado se e somente se as únicas extensões fortemente separáveis de R são da forma $R \oplus \ldots \oplus R$.*

Demonstração: Seja S/R uma extensão fortemente separável. Pelo Lema 1.3.3, S se decompõe em uma soma direta de R-subálgebras conexas. Pela Proposição 1.3.4, tais subálgebras são separáveis. Portanto, S se decompõe em uma soma direta de extensões fortemente separáveis e conexas de R. Sendo R separavelmente fechado, temos que cada somando direto é isomorfo a R. Assim, $S \simeq R \oplus \ldots \oplus R$. A recíproca é imediata. ■

Agora vamos introduzir a definição de fecho separável. A definição dada aqui se aplica apenas para anéis conexos. No entanto, existe uma definição de fecho separável

para um anel não necessariamente conexo, mas esta não será objeto do nosso estudo. O leitor interessado pode consultar os capítulos IV e V de [19].

Definição 1.3.6. *Sejam R um anel conexo e S uma extensão conexa de R. Se S é localmente fortemente separável e separavelmente fechado dizemos que S é um fecho separável para R.*

Lema 1.3.7. *Uma extensão é localmente fortemente separável se e somente se ela é um limite direto de subextensões fortemente separáveis.*

Demonstração: Seja S/R uma extensão localmente fortemente separável. Considere o conjunto diretivo D constituído dos subconjuntos finitos de S com uma ordem parcial dada pela inclusão de conjuntos. Dados $I, J \in D$ com $I \subseteq J$, considere subextensões fortemente separáveis S_I e S_J com $S_I \subseteq S_J$ e $f_{I,J} : S_I \longrightarrow S_J$ a inclusão natural. Então, $\{S_I, f_{I,J}\}$ é um sistema dirigido e $S = \varinjlim S_I$. Por outro lado, está claro que se S é um limite direto de subextensões fortemente separáveis então S é uma extensão localmente fortemente separável. ■

Para a prova da existência do fecho separável de um anel conexo precisamos de alguns resultados auxiliares, os quais serão apresentados a seguir.

Proposição 1.3.8. *[5, Corolário III.2.6] Sejam S uma R-álgebra separável, T/R uma extensão fortemente separável e $f : S \longrightarrow T$ um homomorfismo de R-álgebras. Então $Ker(f)$ é gerado por um idempotente. Em particular, se S é conexo temos que f é um monomorfismo.*

Lema 1.3.9. *Sejam R um anel conexo, T e S extensões localmente fortemente separáveis de R com S um anel conexo e $h : T \longrightarrow S$ um homomorfismo de R-álgebras. Então $Ker(h) = I(x)$, para algum $x \in X(T)$ (ver Definição 1.2.1).*

Demonstração: Seja $t \in Ker(h)$. Como T é uma extensão localmente fortemente separável, existe uma R-subálgebra T' de T com T' uma extensão fortemente separável de R e $t \in T'$. Suponha que $T' = a_1R + \ldots + a_nR$. Como S também é localmente fortemente separável existe uma extensão fortemente separável S' de R tal que $h(a_1), \ldots, h(a_n) \in S'$ e $S' \subseteq S$. Assim, $h(T') \subseteq S'$. Considere então, $\widetilde{h} := h|_{T'} : T' \longrightarrow S'$. Note que, $Ker(\widetilde{h}) = Ker(h) \cap T'$. Pela Proposição 1.3.8, existe um idempotente $e \in T'$ tal que $Ker(\widetilde{h}) = eT'$. Em particular, $h(e) = 0$. Como $t \in T'$ e $h(t) = 0$ temos que $t = t_1e$, para algum $t_1 \in T'$. Assim, $t = te$. Portanto, $Ker(h)$ é gerado por idempotentes. Tome I o ideal de T gerado pelo conjunto de

idempotentes de T que estão em $Ker(h)$. Pela Proposição 1.2.11, para obtermos o resultado desejado é suficiente provar que I é um ideal booleano maximal (ver Definição 1.2.10). Seja $e \in T$ um idempotente. Como S é conexo, $h(e) = 0$ ou $h(e) = 1$ e $h(1-e) = 0$ ou $h(1-e) = 1$. Então, $0 = h(e(1-e)) = h(e)h(1-e)$. Daí, $h(e) = 0$ ou $h(1-e) = 0$, ou seja, e ou $1-e$ está em I mas não ambos. Sejam e e f idempotentes de T com $ef \in I$. Então, $0 = h(ef) = h(e)h(f)$. Novamente pela conexidade de S, temos $h(e) = 0$ ou $h(f) = 0$. Portanto, $e \in I$ ou $f \in I$. Assim, I é um ideal booleano maximal. ■

O resultado anterior pode ser expresso da seguinte maneira: existe $x \in X(T)$ tal que a função induzida $T_x \to S$ é injetora.

Lema 1.3.10. *Sejam R um anel conexo, T uma extensão localmente fortemente separável de R e I um ideal de T gerado por idempotentes. Então $\frac{T}{I}$ também é uma extensão localmente fortemente separável de R.*

Demonstração: Primeiro consideremos o caso em que T é uma extensão fortemente separável de R. Pelo Lema 1.3.3, $T = T_1 \oplus \ldots \oplus T_n$, sendo T_i uma R-álgebra conexa para cada $1 \leq i \leq n$. Portanto, T possui apenas um número finito de idempotentes. Suponha que $I = e_1T + \ldots + e_kT$, onde os $e_i's$ são idempotentes de T. Considere $e = e_1 \oplus \ldots \oplus e_k \in I$, o qual é um idempotente. Para cada $z \in I$ temos $z = e_1a_1 + \ldots + e_ka_k$, $a_j \in T$ para todo $1 \leq j \leq k$. Mas, $ee_i = e_i$. Então, $z = ez \in Te$. Assim, $I \subseteq Te$. A inclusão contrária é imediata. Daí, $I = Te$. Conseqüentemente, $\frac{T}{I} = \frac{T}{Te} \simeq T(1-e)$. Desta forma, $\frac{T}{I}$ é uma extensão fortemente separável. Em geral, como T é uma extensão localmente fortemente separável de R, temos pelo Lema 1.3.7 que $T = \vec{lim}\, T_i$, onde cada T_i é uma subextensão fortemente separável de T. Considere $I_i = I \cap T_i$ e J_i o ideal de T_i gerado pelos idempotentes de I_i. É suficiente provar que $I_i = J_i$. De fato, note que $\frac{T}{I} = \vec{lim}\, \frac{T_i}{I \cap T_i} = \vec{lim}\, \frac{T_i}{I_i} = \vec{lim}\, \frac{T_i}{J_i}$. Pela primeira parte da demonstração, $\frac{T_i}{J_i}$ é uma extensão fortemente separável. Portanto, pelo Lema 1.3.7, $\frac{T}{I}$ é uma extensão localmente fortemente separável de R. Claramente, $J_i \subseteq I_i$. Seja $a \in I_i$. Assim, $a \in I$ e daí, $a = a_1e_1 + \ldots a_re_r$, com $e_j \in I$, $e_j^2 = e_j$ e $a_j \in T$, para todo $1 \leq j \leq r$. Tome $e = e_1 \oplus \ldots \oplus e_r$ e note que $ae = a$. Como $T = \vec{lim}\, T_i$, podemos escolher k tal que $e \in T_k$ e $T_i \subseteq T_k$. Logo, $e \in I \cap T_k = I_k$, ou seja, $e \in J_k$. Pela primeira parte, $\frac{T_k}{J_k}$ é uma extensão fortemente separável de R. Consideremos agora o homomorfismo de R-álgebras $\phi : T_i \longrightarrow \frac{T_k}{J_k}$ dado por: $\phi(x) = x + J_k$. Observe que $z \in Ker(\phi)$ se e somente se $z \in T_i \cap J_k$. Pela Proposição 1.3.8, $Ker(\phi) = \pi T_i$, onde $\pi \in T_i$ é um idempotente. Logo, $\pi \in T_i \cap J_k$.

Então, $\pi = a_1\pi_1 + \ldots + a_s\pi_s$, $a_j \in T_k$, $\pi_j \in I_k = I \cap T_k$ e os $\pi_j's$ são idempotentes. Desta forma, $\pi \in I \cap T_i = I_i$. Como $e \in J_k$ temos $\phi(a) = \phi(ae) = \phi(a)\phi(e) = 0$. Portanto, $a \in Ker(\phi)$, ou seja, $a = \pi b$ para algum $b \in T_i$. Segue que $a \in J_i$, e conseqüentemente, $I_i = J_i$. ■

O próximo resultado é uma caracterização de extensões fortemente separáveis e sua demonstração pode ser vista em [5, Teorema III.2.1].

Lema 1.3.11. *Uma extensão S de R é fortemente separável se e somente se existem uma função R-linear $f : S \longrightarrow R$ e elementos $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tais que:*

i. $\sum_{i=1}^{n} x_i y_i = 1.$

ii. $\sum_{i=1}^{n} x_i f(y_i x) = x$, *para todo* $x \in S$.

Lema 1.3.12. *Sejam $R = \vec{lim}\, R_i$, onde cada R_i é uma subálgebra de R, e S uma extensão fortemente separável de R. Então, para algum l, existe uma extensão fortemente separável S_l de R_l tal que $S \simeq R \otimes_{R_l} S_l$.*

Demonstração: Por hipótese existem elementos $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ e $f \in Hom_R(S, R)$ satisfazendo (i) e (ii) do Lema 1.3.11. Considere o conjunto finito $F = \{f(y_k x_i x_j)\} \cup \{f(y_i y_j)\} \cup \{f(x_j)\} \subseteq R$, onde $1 \leq i, j, k \leq n$. Como $R = \vec{lim}\, R_i$, existe uma R_l subálgebra de R contendo F. Seja S_l o R_l-submódulo de S gerado por $x_1, \ldots, x_n$, ou seja, $S_l = x_1 R_l + \ldots + x_n R_l$. Note que $y_j = \sum_{i=1}^{n} x_i f(y_i y_j) \in S_l$ e $x_i x_j = \sum_{k=1}^{n} x_k f(y_k x_i x_j) \in S_l$. Portanto, S_l é uma R_l-álgebra que contém os elementos $x_1, \ldots, x_n, y_1, \ldots, y_n$. Mais ainda, $f|_{S_l} : S_l \longrightarrow R_l$ é R_l-linear. Então, pelo Lema 1.3.11, S_l é uma extensão fortemente separável de R_l. Considere agora $\mu : R \otimes_{R_l} S_l \longrightarrow S$, $\mu(r \otimes x) = rx$. Observe que μ é um homomorfismo de R_l-álgebras. Dado $z \in S$, temos $z = \sum_{i=1}^{n} x_i f(y_i z)$. Considere $w = \sum_{i=1}^{n} f(y_i z) \otimes x_i \in R \otimes_{R_l} S_l$ e note que $\mu(w) = z$. Logo, μ é sobrejetor. Seja $\gamma = \sum_{i=1}^{n} r_i \otimes s_i \in R \otimes_{R_l} S_l$ com $\sum_{i=1}^{n} r_i s_i = 0$. Então,

$$\gamma = \sum_{i=1}^{n} r_i \otimes s_i = \sum_{i=1}^{n} r_i \otimes \sum_{j=1}^{n} x_j f(y_j s_i) = \sum_{i,j=1}^{n} r_i \otimes x_j f(y_j s_i) =$$

$$\sum_{i,j=1}^{n} r_i f(y_j s_i) \otimes x_j = \sum_{j=1}^{n} f\left(y_j \sum_{i=1}^{n} r_i s_i\right) \otimes x_j = \sum_{j=1}^{n} 0 \otimes x_j = 0.$$

Portanto, μ é um isomorfismo de R_l-álgebras. ■

Enunciaremos outros dois resultados cujas demonstrações podem ser vistas em [5].

Proposição 1.3.13. *[5, Proposição II.1.6] Sejam S_1 e S_2 duas R-álgebras. Se A_i é uma S_i-álgebra separável para $i = 1, 2$ então $A_1 \otimes_R A_2$ é uma $S_1 \otimes_R S_2$-álgebra separável.*

Para uma extensão S/R projetiva e finitamente gerada, dizemos que $rank_R S$ (ou posto de S sobre R) está definido se $rank_{R_P} S_P$ é constante para todo $P \in Spec(R)$. Observe que pela Proposição I.4.1 de [5], S_P é um R_P-módulo livre. Portanto, podemos calcular o seu posto. Se R é conexo, então $rank_R S$ está definido para cada extensão S/R projetiva e finitamente gerada (ver [5, Teorema I.4.12]).

Lema 1.3.14. *[5, Lema III.2.8] Seja S uma extensão fortemente separável de um anel conexo R. Então existe uma extensão fortemente separável T de R tal que T é conexo e $T \otimes S \simeq \underbrace{T \oplus \ldots \oplus T}_{ran_R S - vezes}$*

Dizemos que um R-módulo M é finitamente apresentado se existe uma sequência exata curta de R-módulos $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$ tal que L é um R-módulo livre com base finita e N é finitamente gerado. Note que se S é um R-módulo finitamente gerado e projetivo então S é um R-módulo finitamente apresentado. De fato, suponha que $S = s_1R + \ldots + s_kR$, com $s_i \in S$. Então, $\phi : R^k \longrightarrow S$ dada por $\phi((r_1, \ldots, r_k)) = \sum_{i=1}^{k} r_i s_i$ é um homomorfismo de R-módulos sobrejetor. Portanto, a sequência de R-módulos $0 \longrightarrow Ker(\phi) \longrightarrow R^k \longrightarrow S \longrightarrow 0$ é exata. Como S é um R-módulo projetivo, temos que $Ker(\phi)$ é um somando direto de R^k. Desta forma, $Ker(\phi)$ é um R-módulo finitamente gerado. Daí, S é um R-módulo finitamente apresentado.

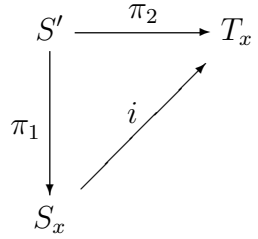
Proposição 1.3.15. *[19, Proposição II.24] Sejam $x \in X(R)$ e S_0 uma R_x-álgebra a qual é um R_x-módulo finitamente apresentado. Então existem uma R-álgebra S a qual é um R-módulo finitamente apresentado tal que $S_x = S_0$. Se S_0 é um R_x-módulo projetivo então S pode ser escolhido projetivo. Se S_0 é uma R_x-álgebra separável então S pode ser escolhida separável.*

Agora estamos em condições de provar a existência do fecho separável para um anel comutativo com unidade e conexo.

Teorema 1.3.16. *Qualquer anel comutativo com unidade e conexo R possui um fecho separável.*

Demonstração: Denotaremos por $S(R) = \{S_i : i \in I\}$ o conjunto das extensões fortemente separáveis de R, com as extensões isomorfas identificadas. Seja $S = \otimes_{i\in I} S_i$. Lembremos que o produto tensorial infinito é definido como segue: seja $\Im = \{F \subseteq I : F \text{ é finito}\}$ e para cada $F \in \Im$ tome $S_F = \otimes_{i\in F} S_i$. Como $\Im$ é um conjunto diretivo por inclusão, definimos $\otimes_{i\in I} S_i = \vec{lim}\, S_F$. Tomemos $x \in X(S)$ e mostremos que S_x é um fecho separável para R. Notemos inicialmente que pelo Teorema 1.2.12, S_x é conexo. Além disso, S_x é uma extensão localmente fortemente separável de R. De fato, note que pela Proposição 1.3.13 temos que S_F é uma R-álgebra separável. Daí, S_F é uma extensão fortemente separável de R. Então, pelo Lema 1.3.7, S é uma extensão localmente fortemente separável de R. Conseqüentemente, pelo Lema 1.3.10, S_x é uma extensão localmente fortemente separável de R. Falta verificar que S_x é separavelmente fechado. Para tanto, considere uma extensão conexa e fortemente separável T_0 de S_x. Pela Proposição 1.3.15, existe uma extensão fortemente separável T de S tal que $T_x = T_0$. Pelo Lema 1.3.12, existe $F \in \Im$ e uma extensão fortemente separável T_F de S_F tal que $T = S \otimes_{S_F} T_F$. Se $S' = \otimes_{I-F} S_i$ então $S = S' \otimes_R S_F$ e $T = S' \otimes_R S_F \otimes_{S_F} T_F \simeq S' \otimes_R T_F$. Verifiquemos que se A é uma extensão fortemente separável de R de posto n então $A \otimes_R S' \simeq \underbrace{S' \times S' \times \ldots \times S'}_{n-vezes}$. De fato, pelo Lema 1.3.14, existe uma extensão fortemente separável S_k de R com $S_k \otimes_R A = \underbrace{S_k \times \ldots \times S_k}_{n-vezes}$. Se $S'' = \bigotimes_{i\in I-F,\, i\neq k} S_i$ então $S' = S'' \otimes_R S_k$ e $A \otimes_R S' = A \otimes_R S'' \otimes_R S_k \simeq S'' \otimes_R (S_k \times \ldots \times S_k) \simeq \underbrace{S' \times \ldots \times S'}_{n-vezes}$. Em particular, $S = S' \otimes_R S_F \simeq \underbrace{S' \times \ldots \times S'}_{rank_R S_F - vezes}$ e $T = S' \otimes_R T_F \simeq \underbrace{S' \times \ldots \times S'}_{rank_R T_F - vezes}$. Então, $S_x = \frac{S}{I(x)} \simeq \frac{S'}{I(x)\cap S'} \times \ldots \times \frac{S'}{I(x)\cap S'}$. Como S_x é conexo, temos $S_x \simeq \frac{S'}{I(x)\cap S'}$. De forma análoga, como T_x é conexo, temos $T_x \simeq \frac{S'}{(I(x)T)\cap S'}$. Conseqüentemente, temos as projeções naturais $\pi_1 : S' \longrightarrow S_x$ e $\pi_2 : S' \longrightarrow T_x$. Identificando S_x com $S_x.1 \subseteq T_x$

temos o seguinte diagrama comutativo



sendo i é a função inclusão. Da sobrejetividade de π_2 temos que i é um isomorfismo. Portanto, $S_x = T_x$. Logo, S_x é separavelmente fechado. Desta forma, S_x é um fecho separável para R. ■

Veremos a seguir que o fecho separável é único, a menos de isomorfismo. Por isso, denotaremos por Ω_R um fecho separável de R. Antes porém, consideremos alguns resultados auxiliares.

Lema 1.3.17. *[14, Lema 1.3] Sejam A uma R-álgebra conexa e S/R uma extensão fortemente separável e conexa. Então existem no máximo $rank_R S$ homomorfimos de R-álgebras distintos de S para A.*

Corolário 1.3.18. *Sejam R um anel conexo, Ω_R um fecho separável para R e S uma extensão fortemente separável de R. Então existem exatamente $rank_R S$ homomorfismos de R-álgebras de S para Ω_R. Quando S é conexo estes homomorfismos são monomorfismos.*

Demonstração: Se S é uma extensão fortemente separável de R então $S \otimes_R \Omega_R$ é uma extensão fortemente separável de Ω_R. Pelo Lema 1.3.3, $S \otimes_R \Omega_R$ se decompõe numa soma direta finita de componentes conexas. Como Ω_R é separavelmente fechado, tais componentes conexas devem ser isomorfas a Ω_R. Portanto, $S \otimes_R \Omega_R \simeq \underbrace{\Omega_R \oplus \ldots \oplus \Omega_R}_{rank_R S - vezes}$. Considere $\pi_i : S \otimes_R \Omega_R \longrightarrow \Omega_R$ a projeção sobre a i-ésima componente. Tome $\sigma_i = \pi_i \mid_{S \otimes_R 1}$ e observe que $S \otimes_R 1 \simeq S$. Então, existem $rank_R S$-homomorfismos de S para Ω_R. Pelo Lema 1.3.17, estes são todos os homomorfismos possíveis de S para Ω_R. Por hipótese, $S = s_1 R + \ldots + s_r R$. Para cada $1 \leq i \leq rank_R S$, seja L_i/R uma subextensão fortemente separável de Ω_R tal que $\sigma_i(s_j) \in L_i$ para todo $1 \leq j \leq r$. Daí, $\sigma_i(S) \subseteq L_i$ para todo $1 \leq i \leq rank_R S$. Pelo Proposição 1.3.8, se S é conexo então σ_i é injetor. ■

Agora vamos provar que o fecho separável é único a menos de isomorfismo. Para tanto, usaremos o seguinte lema.

Lema 1.3.19. *Se Ω_R é um fecho separável de R e Ω'_R é uma extensão localmente fortemente separável de R então existe um homomorfismo de R-álgebras de Ω'_R para Ω_R.*

Demonstração: Dado S uma extensão fortemente separável de R, considere $G(S)$ como sendo o conjunto de todos os homomorfismos de álgebras de S para Ω_R. Pelo Corolário 1.3.18, $G(S)$ é finito. Podemos então introduzir a topologia discreta em $G(S)$ obtendo um espaço topológico compacto e de Hausdorff. Note que se T é outra extensão fortemente separável de R, $T \subseteq \Omega'_R$ e $T \subseteq S$ então a restrição é uma função contínua de $G(S)$ para $G(T)$. Denote por D o conjunto formado pelas extensões fortemente separáveis de R munido de uma ordem parcial dada pela inclusão de conjuntos. Então D é um conjunto diretivo. Mais ainda, pelo que vimos acima, para cada $S \in D$ podemos associar um espaço topológico $G(S)$ e se $T \subseteq S$ existe uma função contínua f_{ST} de $G(S)$ para $G(T)$. Note que $\{G(S), f_{ST}\}$ é um sistema de limite inverso (Ver [5, pg.101]). Desta forma, podemos considerar $\overleftarrow{lim}\ G(S)$. Pelo Lema III.3.2 de [5] , $\overleftarrow{lim}\ G(S) \neq \emptyset$. Sejam $\overline{\sigma} \in \overleftarrow{lim}\ G(S)$ e $x \in \Omega'_R$. Tome S uma extensão fortemente separável de R tal que $x \in S$. Suponha que a imagem de projeção de $\overline{\sigma}$ em $G(S)$ é σ. Defina $h(x) = \sigma(x)$. Assim, h é um homomorfismo de R-álgebras de Ω'_R para Ω_R. ■

Teorema 1.3.20. *O fecho separável é único, a menos de isomorfismo.*

Demonstração: Sejam Ω_R e Ω'_R fechos separáveis para R. Pelo Lema 1.3.19, existe um homomorfismo de R-álgebras $f : \Omega_R \longrightarrow \Omega'_R$ e $g : \Omega'_R \longrightarrow \Omega_R$. Provaremos que cada endomorfismo σ de Ω_R é um automorfismo. Em particular, teremos que f e g são inversos um do outro. Tome $x \in Ker(\sigma)$ e S uma extensão fortemente separável de R ($S \subseteq \Omega_R$) tal que $x \in S$. Pelo Corolário 1.3.18, $x = 0$. Conseqüentemente, σ é injetor. Sejam $y \in \Omega_R$ e T uma extensão fortemente separável de R, $T \subseteq \Omega_R$ e $y \in T$. Pelo Corolário 1.3.18, podemos supor que $f_1, \ldots, f_n$ são todas as imersões de T em Ω_R, onde $n = rank_R T$. Assuma que $f_1(t) = t$ para todo $t \in T$. Note que, $\{\sigma \circ f_1 \ldots, \sigma \circ f_n\} = \{f_1, \ldots, f_n\}$. Portanto, existe $j \in \{1, \ldots, n\}$ tal que $\sigma \circ f_j = f_1$. Logo, $y = f_1(y) = \sigma(f_j(y))$. Assim, σ é sobrejetor. Desta forma, σ é um isomorfismo. Como σ foi escolhido arbitrariamente, temos que $g \circ f$ é um isomorfismo. Conseqüentemente, $\Omega_R \simeq \Omega'_R$. ■

Devido ao teorema acima, diremos **o fecho separável de** R ao invés de **um fecho separável de** R.

Uma extensão de anéis S/R é dita normal se $S^G = R$, onde $G = Aut_R S$ e $S^G = \{s \in S \ : \ \sigma(s) = s \ \text{ para qualquer } \sigma \in G\}$. Finalizamos este capítulo reproduzindo o Corolário III.3.5 de [5] que afirma que Ω_R/R é uma extensão normal de anéis.

Teorema 1.3.21. *Seja Ω_R o fecho separável de um anel conexo R. Se $x \in \Omega_R - R$ então existe $\sigma \in Aut_R(\Omega_R)$ com $\sigma(x) \neq x$.*

Capítulo 2

Teorema do Elemento Primitivo

Nesse capítulo, estudamos o problema da existência de elemento primitivo para extensões fortemente separáveis de anéis. Inicialmente reduzimos este estudo para uma extensão do tipo S/R com R um anel conexo. Em seguida, encontramos condições necessárias e suficientes para que a extensão S/R possua elemento primitivo. Tal resultado pode ser reformulado quando consideramos extensões galoisianas. Finalizamos o capítulo, analisando extensões fortemente separáveis de um LG-anel.

2.1 Redução ao Caso Conexo

Como comentamos acima, podemos reduzir o problema da existência de elemento primitivo para uma extensão fortemente separável S/R, considerando R conexo. Este é o objetivo desta seção. Para tanto, utilizamos alguns argumentos envolvendo propriedades do espectro booleano.

Iniciamos definindo quando uma extensão de anéis comutativos possui elemento primitivo.

Definição 2.1.1. *Dada uma extensão de anéis S/R, dizemos que S/R possui elemento primitivo se existe $\alpha \in S$ tal que $S = R[\alpha]$.*

No restante desta seção, usaremos as notações e os resultados do Capítulo 1. Sejam R um anel comutativo, $X(R)$ seu espectro booleano e $x \in X(R)$. Então, pelo Teorema 1.2.12, $R_x = \frac{R}{I(x)}$ é um anel conexo. Desta forma, o próximo teorema nos remete a estudar o problema da existência de elemento primitivo para uma extensão fortemente separável S/R, no caso em que R é um anel conexo.

Teorema 2.1.2. *Sejam R um anel comutativo com unidade e S uma extensão finitamente gerada de R. Então, S/R possui elemento primitivo se e somente se S_x/R_x possui elemento primitivo para qualquer $x \in X(R)$.*

Demonstração: Suponha que $S = R[\alpha]$, para algum $\alpha \in S$. Como $R_x = \frac{R}{I(x)}$ e $S_x = \frac{S}{I(x)S}$, temos $S_x = R_x[\alpha_x]$. Reciprocamente, dado $x \in X(R)$ temos por hipótese que S_x/R_x tem elemento primitivo. Portanto, existe $\beta = \beta(x) \in S$ (β depende de x) tal que $S_x = R_x[\beta_x]$. Sejam $y_1, \ldots, y_n \in S$ tais que $S = y_1R + \ldots + y_nR$. Então, $(y_i)_x \in S_x = R_x[\beta_x]$, para qualquer $1 \leq i \leq n$. Desta forma, $(y_i)_x = g_i(\beta_x) = g_i(\beta)_x$, onde $g_i \in R[X]$ para todo $1 \leq i \leq n$. Pela Proposição 1.2.8, existe $e_i \in B(R)$ e uma vizinhança $N(e_i)$ de x tal que a igualdade acima continua válida nesta vizinhança e $y_ie_i = g_i(\beta)e_i$ para todo $1 \leq i \leq n$. Tome $e = e_1e_2 \ldots e_n$. Note que, $y_ie = g_i(\beta)e$ para todo $1 \leq i \leq n$. Assim, $Se = R[\beta]e$. Mais ainda, pela Proposição 1.2.6, $N(e) = N(e_1) \cap \ldots \cap N(e_n)$. Portanto, $N(e)$ é uma vizinhança de x. Para cada $x \in X(R)$, obtivemos uma vizinhança $N(e)$ de x. Logo, $X(R)$ é coberto por tais vizinhanças. Pelo Corolário 1.2.4, podemos extrair uma subcobertura finita disjunta $N(f_1), \ldots, N(f_r)$ e elementos $\beta_1, \ldots, \beta_r \in S$ tais que $Sf_i = R[\beta_i]f_i$ para todo $1 \leq i \leq r$. Novamente pela Proposição 1.2.6, temos $f_if_j = 0$ se $i \neq j$ e $f_1 + \ldots + f_r = 1$. Daí, tomando $\alpha = \beta_1f_1 + \ldots + \beta_rf_r$, temos $S = R[\alpha]$. Portanto, a extensão S/R tem elemento primitivo. ■

2.2 Extensões Fortemente Separáveis

A seção anterior remete o problema de encontrar elemento primitivo para uma extensão finitamente gerada S/R de anéis, para o caso em que R é conexo. Por isso, em toda essa seção, R denotará um anel conexo. Consideraremos extensões fortemente separáveis de R e encontraremos condições necessárias e suficientes para que tal extensão possua elemento primitivo.

Definição 2.2.1. *Dado um anel R e um polinômio mônico $g \in R[X]$, dizemos que g é irredutível se para $g = uv$ com $u, v \in R[X]$ polinômios mônicos temos $u = 1$ ou $v = 1$. Quando g não é irredutível, dizemos que g é redutível.*

O próximo lema caracteriza quando um polinômio mônico e separável sobre um anel conexo é irredutível. Este resultado é essencial para a demonstração da próxima proposição.

Lema 2.2.2. *Sejam R um anel conexo e $f(X) \in R[X]$ um polinômio separável em $R[X]$. Então, $\frac{R[X]}{(f)}$ é um anel conexo se e somente se $f(X)$ é irredutível em $R[X]$.*

Demonstração: Assuma que $\frac{R[X]}{(f)}$ é um anel conexo. Suponha também que f é redutível, isto é, $f = gh$, com $g(X), h(X) \in R[X]$ polinômios mônicos e de grau maior ou igual a 1. Pelo Lema 1.2 de [11], g e h são comaximais, isto é, $(g) + (h) = R[X]$. Então, pelo teorema do resto Chinês, $\frac{R[X]}{(f)} \simeq \frac{R[X]}{(g)} \oplus \frac{R[X]}{(h)}$, contradizendo a conexidade de $\frac{R[X]}{(f)}$. Logo, f é irredutível. Reciprocamente, assuma que f é irredutível e que Ω_R é o fecho separável de R. Tome $\alpha \in \Omega_R$ tal que $f(\alpha) = 0$. Defina $\Psi : R[X] \longrightarrow R[\alpha]$ por: $\Psi(t(X)) = t(\alpha)$. Note que $\frac{R[X]}{Ker(\Psi)} \simeq R[\alpha]$ é uma R-álgebra separável. De fato, como $\frac{R[X]}{Ker(\Psi)} \simeq R[\alpha]$ é imagem homomórfica de $\frac{R[X]}{(f)}$, segue do Proposição 1.3.4, que $\frac{R[X]}{Ker(\Psi)} \simeq R[\alpha]$ é uma R-álgebra separável. Assim, $R[\alpha]$ é uma R-álgebra separável. Como $\alpha \in \Omega_R$ e Ω_R é o fecho separável de R, existe uma extensão fortemente separável L de R, com $L \subseteq \Omega_R$ e $\alpha \in L$. Desta forma, $R[\alpha] \subseteq L$. Pela Proposição 1.5 de [14], $R[\alpha]$ é uma extensão fortemente separável de R. Pelo Teorema 2.9 de [14], $Ker(\Psi)$ é um ideal principal de $R[X]$ gerado por um polinômio separável. Mas como $f \in Ker(\Psi)$ e é irredutível, temos $(f) = Ker(\Psi)$. Conseqüentemente, $\frac{R[X]}{(f)} \simeq R[\alpha] \subseteq \Omega_R$. Logo, $\frac{R[X]}{(f)}$ é um anel conexo. ■

A próxima proposição caracteriza quando uma extensão fortemente separável e conexa tem elemento primitivo.

Proposição 2.2.3. *[21, Teorema 3.3] Sejam S/R uma extensão fortemente separável e conexa e $\alpha \in S$. As seguintes afirmações são equivalentes:*

i. Existe um polinômio mônico $f(X) \in R[X]$ tal que $\frac{R[X]}{(f)} \simeq S$ e $f(\alpha) = 0$.

ii. $R[\alpha] = S$.

Demonstração: $(i \rightarrow ii)$ Como S é conexo, pelo Lema 2.2.2, f é irredutível. Então, da mesma maneira que na demonstração do Lema 2.2.2, temos $\frac{R[X]}{(f)} \simeq R[\alpha]$. Por hipótese, $\frac{R[X]}{(f)} \simeq S$. Daí, $R[\alpha] \simeq S$. Portanto, $ran_R R[\alpha] = rank_R S$. Pelo Lema 1.1 de [9], $R[\alpha] = S$.

$(ii \rightarrow i)$ Suponha que $rank_R S = n$. Pelo Teorema III.3.6 de [5], $S = (\Omega_R)^H$, onde H é um subgrupo de $G = Aut_R(\Omega_R)$ e $[G : H] = n$. Assuma que $\sigma_1 = 1, \ldots, \sigma_n$ são os representantes distintos das classes laterais de H em G e que $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma_j(\alpha) : \ j = 1, \ldots, n\}$. Considere $f(X) = (X - \alpha_1) \ldots (X - \alpha_n)$ e note que $\sigma(f) = f$ para cada $\sigma \in G$. Portanto, os coeficientes de f são invariantes pela ação de G. Daí,

usando o Teorema 1.3.21, temos que $f \in R[X]$. Conforme a demonstração do Lema 2.7 de [14], f é um polinômio separável em $R[X]$. Além disso, G é transitivo sobre o conjunto das raízes de f, isto é, dadas duas raízes α, β de f existe um elemento $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Assim, pelo Lema 1.5 de [11], f é irredutível. Novamente, como na demonstração do Lema 2.2.2, temos $\frac{R[X]}{(f)} \simeq R[\alpha] = S$. ■

Seja S/R uma extensão fortemente separável. Pelo Lema 1.3.3, $S = S_1 \oplus S_2 \oplus \ldots \oplus S_r$, onde cada S_j é uma R-álgebra conexa. Suponha que para cada j, e_j é a unidade de S_j. Note que $e_i e_j = 0$ para $i \neq j$. Suponha também que $1 = a_1 + a_2 + \ldots + a_r$ com $a_j \in S_j$ para cada $1 \leq j \leq r$. Então, $e_j = 1e_j = a_1e_j + a_2e_j + \ldots + a_je_j + \ldots + a_re_j$. Como $a_ie_j = a_ie_ie_j = 0$ se $i \neq j$, temos $e_j = a_je_j = a_j$. Desta forma, $1 = e_1 + \ldots + e_r$. Denotaremos por I_j o conjunto dos polinômios mônicos $f \in R[X]$ tais que $\frac{R[X]}{(f)} \simeq S_j$. Observe que se $f \in I_j$ então f é irredutível, separável e $\partial f = rank_R S_j$. Pela proposição acima, existem $\alpha_j \in S_j$ e $f_j \in I_j$ tal que $f_j(\alpha_j) = 0$ se e somente se $S_j = R[\alpha_j]$. Usaremos estas notações no próximo teorema.

Teorema 2.2.4. *A extensão fortemente separável $S = S_1 \oplus \ldots \oplus S_r/R$ tem elemento primitivo se e somente se para cada $1 \leq j \leq r$ existe $f_j \in I_j$ tal que $(f_i) + (f_j) = R[X]$ $(i \neq j)$. Além disso, se $\alpha_j \in S_j$ e $f_j(\alpha_j) = 0$ para cada $1 \leq j \leq r$ então $\alpha = \alpha_1e_1 + \ldots + \alpha_re_r$ é elemento primitivo de S/R.*

Demonstração: Seja $\alpha \in S$ tal que $S = R[\alpha]$. Tome $\alpha_j \in S_j$ tal que $\alpha = \alpha_1 + \ldots + \alpha_r$. Note que, $\alpha e_j = \alpha_j e_j$ para todo $1 \leq j \leq r$. Assim, $R[\alpha_j] = R[\alpha_j]e_j = R[\alpha_j e_j]e_j = R[\alpha e_j]e_j = R[\alpha]e_j = Se_j = S_je_j = S_j$. Pela Proposição 2.2.3, existe um polinômio mônico $f_j \in R[X]$ tal que $f_j(\alpha_j) = 0$ e $\frac{R[X]}{(f_j)} \simeq S_j$ para todo $1 \leq j \leq r$. Logo, obtemos um isomorfismo Ψ de $R[\alpha]$ em $\frac{R[X]}{(f_1)} \times \ldots \times \frac{R[X]}{(f_r)}$ dado por: $\Psi(h(\alpha)) = (h(X) + (f_1), h(X) + (f_2), \ldots, h(X) + (f_r))$. De fato, observe que $\frac{R[X]}{(f_1)} \times \ldots \times \frac{R[X]}{(f_r)} \simeq S_1 \times \ldots \times S_r \simeq S_1 \oplus \ldots \oplus S_r = S = R[\alpha]$. Se $\phi : R[X] \longrightarrow R[\alpha]$ é o homomorfismo que leva $h(X)$ em $h(\alpha)$ então $\Psi \circ \phi : R[X] \longrightarrow \frac{R[X]}{(f_1)} \times \ldots \times \frac{R[X]}{(f_r)}$ é dado por: $\Psi \circ \phi(h(X)) = (h(X) + (f_1), h(X) + (f_2), \ldots, h(X) + (f_r))$. Mais ainda, $\Psi \circ \phi$ é sobrejetor. Pelo teorema do resto Chinês, $(f_i) + (f_j) = R[X]$, sempre que $i \neq j$.

Reciprocamente, suponha que existe $f_j \in I_j$ tal que se $i \neq j$ então $(f_i) + (f_j) = R[X]$ para cada $1 \leq i, j \leq r$. Pelo teorema do resto Chinês temos, $S = S_1 \oplus \ldots \oplus S_r \simeq S_1 \times \ldots \times S_r \simeq \frac{R[X]}{(f_1)} \times \ldots \times \frac{R[X]}{(f_r)} \simeq \frac{R[X]}{(f_1 \ldots f_r)}$. Logo, S/R tem elemento primitivo. Para finalizar, assuma que $\alpha_j \in S_j$ e que $f_j(\alpha_j) = 0$. Pela Proposição 2.2.3, $S_j = R[\alpha_j]$. Tome $\alpha = \alpha_1 + \ldots + \alpha_r$ e note que o isomorfismo acima leva $X + (f_1 \ldots f_r)$ em α.

Portanto, α é um elemento primitivo da extensão S/R. ■

Observe que, pelo teorema acima, se uma das subálgebras conexas de R não possui elemento primitivo então S/R não possui elemento primitivo. No entanto, cada componente conexa possuir elemento primitivo não é uma condição suficiente para que S/R possua elemento primitivo. Além disso, precisamos impor a condição de comaximalidade entre os polinômios f_j. O próximo exemplo ilustra e enfatiza este fato.

Exemplo: A extensão de anéis $S = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z}$ é fortemente separável e não possui elemento primitivo. De fato, se $S/\mathbb{Z}$ tivesse elemento primitivo então $\frac{S}{\mathcal{M}S}/\frac{\mathbb{Z}}{\mathcal{M}}$ o teria, para cada $\mathcal{M} \in Max(\mathbb{Z})$. Mas é fácil ver que $\frac{S}{\mathcal{M}S}/\frac{\mathbb{Z}}{\mathcal{M}}$ não tem elemento primitivo se $\mathcal{M} = 2\mathbb{Z}$. Claramente existem $f_1, f_2, f_3 \in \mathbb{Z}[X]$ polinômios distintos tais que $\frac{\mathbb{Z}[X]}{(f_i)} \simeq \mathbb{Z}$ para $i = 1, 2, 3$. Vamos verificar que não existem três polinômios comaximais de grau 1 em $\mathbb{Z}[X]$. Suponha que $f_i(X) = X - a_i$ com $a_i \in \mathbb{Z}$ e que $(f_i) + (f_j) = \mathbb{Z}[X]$. Então, existem $i, j \in \{1, 2, 3\}$ tais que $|a_i - a_j| \geq 2$, pois os polinômios f_i's são distintos. Pelo teorema do resto Chinês, se $f = f_1 f_2 f_3 \in \mathbb{Z}[X]$ então $\frac{\mathbb{Z}[X]}{(f)} \simeq \frac{\mathbb{Z}[X]}{(f_1)} \oplus \frac{\mathbb{Z}[X]}{(f_2)} \oplus \frac{\mathbb{Z}[X]}{(f_3)} \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. Portanto, f é um polinômio separável em $\mathbb{Z}[X]$. Pelo Teorema 2.3 de [25], $\delta(f) = (a_1 - a_2)^2(a_1 - a_3)^2(a_2 - a_3)^2 \in U(\mathbb{Z})$. Desta forma, $a_i - a_j \in U(\mathbb{Z})$, o que é um absurdo.

Agora, consideraremos um corolário do teorema acima. Antes porém, precisamos da seguinte definição.

Definição 2.2.5. *Uma extensão de anéis S/R é dita trivial se $S = R \oplus \ldots \oplus R$.*

Note que se S/R é trivial então S é um R-módulo projetivo e S é uma R-álgebra separável. Além disso, claramente S é um R-módulo finitamente gerado. Portanto, toda extensão trivial é uma extensão fortemente separável.

Corolário 2.2.6. *Sejam R um anel conexo e S/R uma extensão trivial. Então S/R possui elemento primitivo se e somente se existem $n = rank_R S$ elementos $r_1, \ldots, r_n \in R$ tais que $r_i - r_j \in U(R)$.*

Demonstração: Sejam $r_1, \ldots, r_n \in R$ tais que $r_i - r_j \in U(R)$ se $i \neq j$. Considere $f_i = (X - r_i) \in R[X]$. Pelo Teorema 2.2.4, é suficiente provar que $(f_i) + (f_j) = R[X]$ se $i \neq j$. Observe que, $r_i - r_j \in (f_i) + (f_j)$. Conseqüentemente, $(f_i) + (f_j) = R[X]$. Reciprocamente, assuma que S/R tem elemento primitivo. Pelo Teorema 2.2.4, existem $r_i \in R$ e $f_i \in R[X]$ um polinômio mônico tais que $f_i(r_i) = 0$ e $\frac{R[X]}{(f_i)} \simeq R$.

Portanto, $f_i(X) = X - r_i$. Mais ainda, $(f_i) + (f_j) = R[X]$. Como no exemplo acima temos, $r_i - r_j \in U(R)$. ■

2.3 Extensões Galoisianas

Provaremos nessa seção que, quando S/R é uma extensão galoisiana e R é conexo, as componentes conexas de S são duas a duas isomorfas. Isso permite uma reformulação do Teorema 2.2.4.

Dados uma extensão de anéis S/R, um grupo finito G de $R-$automorfimos de S e um elemento $\alpha \in S$, denotaremos por $G_\alpha = \{\sigma \in G : \sigma(\alpha) = \alpha\}$. Dado $E \subseteq S$, dizemos que G é transitivo sobre E se para quaisquer $x, y \in E$ existe $\sigma \in G$ tal que $\sigma(x) = y$. Dizemos que um idempotente $e \in R$ é primitivo se e não pode ser escrito como soma de dois idempotentes ortogonais não nulos de R. Denotaremos por $I_p(S)$ o conjunto dos idempotentes primitivos de S.

O próximo resultado generaliza o Lema 1.1 de [17].

Lema 2.3.1. *Sejam R um anel conexo e S/R uma extensão galoisiana com grupo G. Então:*

i. $I_p(S) \neq \emptyset$ e G é transitivo sobre $I_p(S)$. Mais ainda, para todo $e, e' \in I_p(S)$ temos $G_e|_{Se} \simeq G_e \simeq G_{e'}$, $|G| = |G_e|\,(\#I_p(S))$, Se/Re é uma extensão galoisiana com grupo $(G_e|_{Se})$, Se é um anel conexo e $Se \simeq Se'$.

ii. Se_i, $1 \leq i \leq r$, são as únicas (a menos de isomorfismo) R-subálgebras maximais, separáveis e conexas de S.

Demonstração: (i) Pelo Lema 2.14 de [13], $I_p(S) \neq \emptyset$. Seja $e \in I_p(S)$ e considere $\{\sigma(e) : \sigma \in G\} = \{\sigma_1(e) = e_1, \ldots, \sigma_r(e) = e_r\}$, com $\sigma_1 = Id$ e $e_i \neq e_j$ $(i \neq j)$. Note que $e_i^2 = e_i$ e $e_i \in I_p(S)$ para todo $1 \leq i \leq r$. Mas se $e, e' \in I_p(S)$ então $ee' = 0$. De fato, suponha que $ee' \neq 0$ e note que $e = ee' + (e - ee')$. Pela nossa suposição, $ee' \neq 0$. Se $e = ee'$ então $e' = e + (e' - e)$, $e \neq 0$, $e' - e \neq 0$ e $e(e' - e) = 0$. Isto é uma contradição, pois $e' \in I_p(S)$. Logo, $e - ee' \neq 0$. Portanto, e é uma soma de dois idempotentes ortogonais não nulos. Novamente temos uma contradição, pois $e \in I_p(S)$. Conseqüentemente, $e_i e_j = 0$ se $i \neq j$. Tomando $f = e_1 + \ldots + e_r$, temos $f^2 = (e_1 + \ldots + e_r)(e_1 + \ldots + e_r) = (e_1 + \ldots + e_r) = f$ e $\sigma(f) = f$ para todo $\sigma \in G$. Assim, f é um idempotente de $S^G = R$. Como R é conexo, temos $f = 0$ ou $f = 1$. Se $f = 0$ então $0 = e_j \cdot 0 = e_j(e_1 + \ldots + e_r) = e_j$, para cada $1 \leq j \leq r$. Mas isto

é um absurdo. Daí, $f = 1$. Assim, para cada $e \in I_p(S)$, temos $e = ee_1 + \ldots + ee_r$. Se $e \notin \{e_1, \ldots, e_r\}$ então $ee_i = 0$. Conseqüentemente, $e = 0$ o que é um absurdo. Desta forma, $I_p(S) \subseteq \{e_1, \ldots, e_r\}$. Como a inclusão contrária é imediata, temos $I_p(S) = \{e_1, \ldots, e_r\}$. Dessa igualdade, segue a transitividade de G sobre $I_p(S)$.

Verifiquemos agora que Se/Re é uma extensão galoisiana com grupo $(G_e|_{Se})$. Pela Definição 1.1.4, é suficiente provar que $(Se)^{(G_e|_{Se})} = Re$ e que existem $z_i, w_i \in Se$ $(i = 1, \ldots, n)$ tais que $\sum_{i=1}^{n} z_i\sigma(w_i) = \delta_{1,\sigma} = \begin{cases} e, & \text{se } \sigma|_{Se} = 1 \\ 0, & \text{se } \sigma|_{Se} \neq 1, \text{ para todo } \sigma \in G_e \end{cases}$. Claramente, $Re \subseteq (Se)^{(G_e|_{Se})}$. Tome $\alpha \in (Se)^{(G_e|_{Se})}$ e considere $\alpha_i = \sigma_i(\alpha)$ $(i = 1, \ldots, r)$ e $b = \alpha_1 + \ldots + \alpha_r$. Seja $\sigma \in G$ tal que $\sigma(e_i) = e_j$. Então, $\sigma(\sigma_i(e)) = e_j = \sigma_j(e)$. Assim, $\sigma_j^{-1}\sigma\sigma_i(e) = e$. Daí, podemos considerar $\sigma_j^{-1}\sigma\sigma_i \in (G_e|_{Se})$. Logo, $\sigma_j^{-1}\sigma\sigma_i(\alpha) = \alpha$, ou seja, $\sigma(\alpha_i) = \alpha_j$. Pela escolha de b, temos $\sigma(b) = b$, para todo $\sigma \in G$. Como $S^G = R$, temos que $b \in R$. Observe que $\alpha = se$ para algum $s \in S$. Logo, $\alpha e = \alpha$. Mais ainda, $be = \sigma_1(\alpha)e + \sigma_2(\alpha)e + \ldots + \sigma_r(\alpha)e = \alpha e + \sigma_2(s)\sigma_2(e)e + \ldots + \sigma_r(s)\sigma_r(e)e = \alpha e + \sigma_2(s)e_2e + \ldots + \sigma_r(s)e_re = \alpha e = \alpha$. Então, $\alpha \in Re$ e $(Se)^{(G_e|_{Se})} = Re$. Por hipótese, existem $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tais que $\sum_{i=1}^{n} x_i\sigma(y_i) = \delta_{1,\sigma}$. Tomando $z_i = x_ie$ e $w_i = y_ie$, para cada $\sigma \in (G_e|_{Se})$, temos

$$\sum_{i=1}^{n} z_i\sigma(w_i) = \sum_{i=1}^{n} x_ie\sigma(y_ie) = \begin{cases} e & , \text{ se } \sigma = Id_{(G_e|_{Se})} \\ 0 & , \text{ se } \sigma \neq Id_{(G_e|_{Se})} \end{cases}.$$

Logo, Se/Re é uma extensão galoisiana com grupo $(G_e|_{Se})$.

Note também que temos os seguintes isomorfismos: $R \simeq Re_i$ $(r \longmapsto re_i)$, $Re \simeq Re_i$ $(re \longmapsto \sigma_i(re) = re_i)$ e $Se \simeq Se_i$ $(se \longmapsto \sigma_i(se) = \sigma_i(s)e_i)$, para todo $1 \leq i \leq r$. Considere $\phi : G_e \longrightarrow G_e|_{Se}$ dada por $\phi(\sigma) = \sigma|_{Se}$. É fácil ver que ϕ é um homomorfismo sobrejetor de grupos. Suponha que $\phi(\sigma) = Id_{(G_e|_{Se})}$. Então, $\sigma \in G_e$ e $\sigma(se) = \sigma(s)e = se$ para todo $s \in S$. Mas S/R é uma extensão galoisiana. Portanto, S é G-forte, isto é, para cada idempotente e' não nulo de S e para cada par $\gamma \neq \tau$ em G existe $x \in S$ tal que $\gamma(x)e' \neq \tau(x)e'$. Desta forma, $\sigma = Id_S$. Conseqüentemente, ϕ é injetor. Logo, $(G_e|_{Se}) \simeq G_e$. Assim, como $S = Se_1 \oplus \ldots \oplus Se_r$, temos $|G| = rank_R S = r \cdot rank_{Re} Se = (\#I_p(S))|G_e|$. Para finalizar, observe que se $e, e' \in I_p(S)$ e $\sigma(e) = e'$ então $\Psi : G_e \longrightarrow G_{e'}$, dada por $\Psi(\tau) = \sigma\tau\sigma^{-1}$, é um isomorfismo de grupos.

Falta verificar que Se é um anel conexo. Vamos provar que se S é um anel comutativo com unidade e $e \in S$ é um idempotente primitivo então Se é um anel comutativo com

unidade e conexo. De fato, tome $e' \in Se$ um idempotente. Note que $e = e' + (e - e')$ e que $(e-e')^2 = (e-e')$, pois $e'e = e'$. Mais ainda, $e'(e-e') = 0$. Portanto, podemos escrever o idempotente e como uma soma de dois idempotentes ortogonais. Sendo e um idempotente primitivo, temos $e' = 0$ ou $e' = e$. Assim, Se é um anel comutativo e conexo.

(ii) Seja L uma R subálgebra de S que é maximal em relação a propriedade de ser separável sobre R e conexa. Considere $\phi : L \longrightarrow Le_i$ dada por $\phi(x) = xe_i$. Como vimos na parte (i) deste lema, Se_i/Re_i é uma extensão galoisiana e, conseqüentemente, uma extensão fortemente separável. Note que $R \simeq Re_i \subseteq Le_i \subseteq Se_i$. Como L é uma R-álgebra separável, verifica-se facilmente que Le_i é uma Re_i-álgebra separável. Pela Proposição 1.5 (1) de [14], Le_i é uma extensão fortemente separável de Re_i. Mas, $Re_i \simeq R$. Daí, Le_i é uma extensão fortemente separável de R. Pela conexidade de L e Proposição 1.3.8, obtemos a injetividade de ϕ. A sobrejetividade é clara. Mas, Se_i é um anel conexo. Usando a maximalidade de L e o isomorfismo acima, tem-se $Se_i = Le_i$. ■

Com as notações do Lema 2.3.1, denotaremos por $\mathcal{F}$ o conjunto de subanéis conexos maximais de S contendo R, os quais são extensões separáveis de R. Pelo Lema 2.3.1, se $L \in \mathcal{F}$ então $L \simeq Se_i$, onde $e_i \in I_p(S)$.

Dado um anel conexo R, uma extensão galoisiana S/R e $L \in \mathcal{F}$, denotaremos por $I_R(L)$ o conjunto dos polinômios mônicos $f_i(X) \in R[X]$ tais que $\frac{R[X]}{(f_i)} \simeq L$ e $(f_i) + (f_j) = R[X]$. O teorema abaixo, generaliza a Proposição 1.4 de [17] e é uma reformulação do Teorema 2.2.4 no caso em que a extensão S/R é galoisiana. Sua demonstração, apesar de usar argumentos parecidos com os utilizados no Teorema 2.2.4, será feita.

Teorema 2.3.2. *Sejam R um anel conexo, S/R uma extensão galoisiana com grupo G , $r = \#I_p(S)$ e $L \in F$. Então, S/R possui elemento primitivo se e somente se $\#I_R(L) \geq r$. Mais ainda, se $g_1, \ldots, g_r \in I_R(L)$ são polinômios distintos e $\{c_1, \ldots, c_r\}_r \subseteq L$ com $g_i(c_i) = 0$ então $c = c_1e_1 + \ldots + c_re_r \in S$ é elemento primitivo de S/R e $\prod_{i=1} g_i(X) = \prod_{\sigma \in G}(X - \sigma(c))$.*

Demonstração: Pelo Lema 2.3.1 e sua demonstração, $S = Le_1 \oplus \ldots \oplus Le_r$. Assim, $\alpha = \alpha_1e_1 + \ldots + \alpha_re_r$, $\alpha_i \in L$ para cada $1 \leq i \leq r$. Também pelo Lema 2.3.1, L/R é galoisiana. Seja H o grupo de Galois da extensão L/R. Para cada i, tome $f_i(X) = \prod_{\tau \in H}(X - \tau(\alpha_i))$. Note que, $f_i(\alpha_i) = 0$. Observe que se f_i e f_j forem comaximais então

eles serão naturalmente distintos. De qualquer forma, verifiquemos agora que $f_i \neq f_j$ $(i \neq j)$ e que $f_i \in I_R(L)$. Suponha que $\{f_1, \ldots, f_r\} = \{u_1, \ldots, u_t\}$, $t \leq r$ e $u_i \neq u_j$ $(i \neq j)$. Se $u = u_1 \cdot u_2 \ldots u_t$ então $u(\alpha) = \sum_{i=1}^{r} u(\alpha)e_i = \sum_{i=1}^{r} u(\alpha_i)e_i = 0$. Como α é elemento primitivo de S/R, segue do Lema 1.3 de [17], que $\{1, \alpha, \ldots, \alpha^{mr-1}\}$ é uma R-base de S, onde $m = rank_R L = |H|$. Mas, $u(X) \in R[X]$ e $u(\alpha) = 0$. Daí, $\partial u \geq mr$. Assim, $mr \leq \partial u = mt \leq mr$, ou seja, $r = t$. Também temos, $R[\alpha_i]e_i = R[\alpha]e_i = Se_i = Le_i$. Logo, dado $y \in L$ existe $x \in R[\alpha_i]$ tal que $ye_i = xe_i$. Daí, $(y - x)e_i = 0$. Usando o fato que $\Gamma : L \longrightarrow Le_i$, definida por $\Gamma(x) = xe_i$ é injetora, concluímos que $y = x$. Portanto, $R[\alpha_i] = L$. Como na demonstração do Teorema 2.2.4, $\frac{R[X]}{(f_i)} \simeq R[\alpha_i] = L$. Note que, $\frac{R[X]}{(f_1)} \times \ldots \times \frac{R[X]}{(f_r)} \simeq R[\alpha_1] \times \ldots \times R[\alpha_r] \simeq R[\alpha_1]e_1 \times \ldots \times R[\alpha_r]e_r = S$. Tal isomorfismo é dado por: $\psi(h_1(X) + (f_1), \ldots, h_r(X) + (f_r)) = h_1(\alpha_1)e_1 + \ldots + h_r(\alpha_r)e_r$. Assim, obtemos o seguinte diagrama comutativo,

$$\begin{array}{ccc} R[X] & \xrightarrow{\phi} & \dfrac{R[X]}{(f_1)} \times \ldots \times \dfrac{R[X]}{(f_r)} \\ & \searrow & \wr \downarrow \psi \\ & & R[\alpha] = S \end{array}$$

onde ϕ é o homomorfismo canônico. Portanto, ϕ é sobrejetor. Pelo teorema do resto Chinês, $(f_i) + (f_j) = R[X]$ $(i \neq j)$. Logo, $\#I_R(L) \geq r$.
Reciprocamente, tome $g_1, \ldots, g_r \in I_R(L)$ com $g_i \neq g_j$ $(i \neq j)$. Pelo teorema do resto Chinês, tomando $g = \prod_{i=1}^{r} g_i$, obtemos

$$\frac{R[X]}{(g)} \simeq \frac{R[X]}{(g_1)} \times \ldots \times \frac{R[X]}{(g_r)} \simeq S.$$

Logo, S/R possui um elemento primitivo. Considere $\{c_1, \ldots, c_r\} \subseteq L$ tal que $g_i(c_i) = 0$. Pela Proposição 2.2.3, $L = R[c_i]$ para todo $1 \leq i \leq n$. Observe que, neste caso, o isomorfismo construído acima leva $x = X + (g)$ em $c = c_1e_1 + \ldots + c_re_r$. Pelo Lema 1.3 de [17], $\{1, c, \ldots, c^{mr-1}\}$ é uma R-base de S, onde $m = rank_R L$. Tome $h(X) = \prod_{\sigma \in G}(X - \sigma(c)) \in R[X]$. Então, $\partial h = |G| = mr$. Como g é mônico, pelo algoritmo da divisão, existem $q(X), r(X) \in R[X]$ tais que $h(X) = g(X)q(X) + r(X)$, com $\partial r(X) < \partial g(X)$. Mas, $\partial g(X) = mr$. Desta forma, $r(c) = 0$ e $\partial r(X) <$

mr. Da independência linear do conjunto $\{1, c, \ldots, c^{mr-1}\}$, segue que, $r(X) = 0$. Conseqüentemente, $\partial h(X) = \partial g(X) + \partial q(X)$. Daí, $\partial q(X) = 0$. Portanto, $q(X) = 1$ e $h(X) = g(X)$. ■

Os resultados desta seção nos dizem que uma extensão galoisiana S de um anel conexo R possui elemento primitivo desde que sua componente conexa (as componentes conexas são duas a duas isomorfas neste caso) possua e existam suficientes ($\#I_R(L) \geq \#I_p(S)$) polinômios separáveis e dois a dois comaximais em $R[X]$. No próximo capítulo, dado um polinômio $f \in I_R(L)$ construiremos a partir deste (sob certas condições), polinômios pertencentes a $I_R(L)$.

2.4 Extensões Galoisianas de um LG-anel

Em [17], estuda-se a existência de elemento primitivo de extensões galoisianas de anéis semilocais. Dentre outras coisas prova-se que se S/R é uma extensão galoisiana e $Max(R) = \{\mathcal{M}_1, \ldots, \mathcal{M}_t\}$ então S/R tem elemento primitivo se e somente se $\frac{S}{\mathcal{M}_i S}/\frac{R}{\mathcal{M}_i}$ tem elemento primitivo para todo $1 \leq i \leq t$. Usando os mesmos argumentos utilizados por A. Paques na demonstração do Teorema 2.4 em [26], estendemos este resultado para LG-anéis.

Iniciamos com a definição de LG-anel.

Definição 2.4.1. *Um anel comutativo com unidade R é dito um LG-anel (local-global) se quando um polinômio $f(X_1, \ldots, X_n)$ ($n \in \mathbb{N}$) representa uma unidade sobre $R_{\mathcal{M}}$, para cada ideal maximal $\mathcal{M}$ de R, então f representa uma unidade sobre R.*

Lembre-se que dizemos que o polinômio f representa uma unidade sobre R se existem $a_1, \ldots, a_n \in R$ tais que $f(a_1, \ldots, a_n) \in U(R)$. Note também que cada anel semilocal é um LG-anel. De forma mais geral, anéis os quais são von Neumann regular módulo seu radical de Jacobson são LG-anéis.

Proposição 2.4.2. *Sejam R um LG-anel e S/R uma extensão fortemente separável de posto constante. Então, S/R tem elemento primitivo se e somente se $\frac{S}{\mathcal{M}S}/\frac{R}{\mathcal{M}}$ tem elemento primitivo para cada $\mathcal{M} \in Max(R)$.*

Demonstração: É claro que se S/R possui elemento primitivo então $\frac{S}{\mathcal{M}S}/\frac{R}{\mathcal{M}}$ tem elemento primitivo para cada $\mathcal{M} \in Max(R)$. Reciprocamente, assuma que $\frac{S}{\mathcal{M}S}/\frac{R}{\mathcal{M}}$ tem elemento primitivo, para cada $\mathcal{M} \in Max(R)$. Por hipótese, S é um R-módulo

de posto constante, digamos, $rank_R S = n$. Conforme [28], existe uma extensão galoisiana T/R com grupo de Galois (a menos de isomorfismo) o grupo simétrico G_n (o grupo de todas as permutações de um conjunto finito com n elementos) tal que $S = T^{G_{n-1}}$, onde G_{n-1} é considerado como o subgrupo de G_n que deixa um elemento fixo. Sejam $\sigma_1 = 1, \sigma_2, \ldots, \sigma_n \in G_n$ os representantes distintos das classes laterais de G_{n-1} em G_n. Como R é um LG-anel, segue do Teorema 2.10 de [8], que S é um R-módulo livre. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma R-base de S e $u = u(X_1, \ldots, X_n) = \sum_{i=1}^{n} \alpha_i X_i \in S[X_1, \ldots, X_n] \subseteq T[X_1, \ldots, X_n]$. Pelo Lema 1.7 de [3], $T[X_1, \ldots, X_n] \simeq T \otimes_R R[X_1, \ldots, X_n]$ é uma extensão galoisiana de $R[X_1, \ldots, X_n]$ com grupo de Galois G_n. Então,

$$g(X_1, \ldots, X_n) = \prod_{i=2}^{n} \left[\prod_{j=1}^{n} \sigma_j \left(\sigma_i(u) - u \right) \right]$$

é um polinômio com coeficientes em $R[X_1, \ldots, X_n]$. Sejam $\mathcal{M} \in Max(R)$, $\overline{R} = \frac{R}{\mathcal{M}}$, $\overline{S} = \frac{S}{\mathcal{M}S}$, $\overline{T} = \frac{T}{\mathcal{M}T}$, $\overline{G}_n = \{\overline{\sigma} = \sigma \otimes 1 \ : \ \sigma \in G_n\}$ e $\overline{G}_{n-1} = \{\overline{\sigma} = \sigma \otimes 1 \ : \ \sigma \in G_{n-1}\}$. Claramente, $\overline{T}$ é uma extensão galoisiana de $\overline{R}$ com grupo de Galois $\overline{G}_n$, $\overline{S}$ é uma extensão fortemente separável de $\overline{R}$ de posto n e $\overline{T}^{\overline{G}_{n-1}} = \overline{S}$. Mais ainda, $\overline{\sigma}_1, \ldots, \overline{\sigma}_n$ são representantes distintos para as classes laterais de $\overline{G}_{n-1}$ em $\overline{G}_n$. Por hipótese, existe $\alpha \in S$ tal que $\overline{S} = \overline{R}[\overline{\alpha}]$. Suponha que $\alpha = \sum_{i=1}^{n} \lambda_i \alpha_i$, com $\lambda_i \in R$. Pela Proposição 2.1 de [26], temos $\overline{\sigma}_j(\overline{\alpha}) - (\overline{\alpha}) \in U\left(\overline{T}\right)$, para cada $2 \leq j \leq n$. Conseqüentemente, $\overline{g}(\overline{\lambda}_1 \ldots, \overline{\lambda}_n) = \prod_{i=2}^{n} \left[\prod_{j=1}^{n} \overline{\sigma_j} \left(\overline{\sigma}_i(\overline{\alpha}) - (\overline{\alpha}) \right) \right]$ é uma unidade em $\overline{T}$. Mas, $U\left(\overline{T}\right) \cap \overline{R} = U\left(\overline{R}\right)$. Assim, $\overline{g}(\overline{\lambda}_1, \ldots, \overline{\lambda}_n) \in U\left(\overline{R}\right)$. Portanto, $\overline{g}$ representa uma unidade sobre o corpo residual $\frac{R}{\mathcal{M}}$. Mas isto, é equivalente a dizer que g representa uma unidade sobre $R_{\mathcal{M}}$. Sendo R um LG anel, temos que g representa uma unidade sobre R, ou seja, existem $r_1, \ldots, r_n \in R$ tais que $g(r_1, \ldots, r_n) \in U(R)$. Desta forma, para cada $2 \leq j \leq n$, temos $\sigma_j(u(r_1, \ldots, r_n)) - u(r_1, \ldots, r_n) \in U(T)$. Novamente pela Proposição 2.1 de [26] , $u(r_1, \ldots, r_n)$ é um elemento primitivo de S/R. ■

Observação: O resultado acima não é verdadeiro em geral (mesmo quando o anel R é conexo), conforme o exemplo abaixo extraído de [1].

Exemplo: Sejam K um corpo algebricamente fechado de característica 2 e $B = K[X, Y]$. Tome σ um epimorfismo K-linear de B tal que $\sigma(X) = X+1$, $\sigma(Y) = X^2 + Y + 1$. Note que a ordem de σ é 4. Além disso, $\sigma(X) - 1 = X$ e $(\sigma(X))^2 - \sigma(Y) = Y$. Portanto, $X, Y \in \sigma(B)$. Então, σ é um automorfismo de B. Considere $A = B^{<\sigma>}$

e verifiquemos que B/A é uma extensão galoisiana. Seja $\mathcal{M} \in Max(B)$. Como K é algebricamente fechado, segue como conseqüência do Lema de Normalização de Noether que, $\mathcal{M} = (X-a, Y-b)$. Logo, $\frac{B}{\mathcal{M}} \simeq K$. Note que, $T(\mathcal{M}) = \{\sigma \in Aut_A B \ : \ \sigma(x) - x \in \mathcal{M} \text{ para todo } x \in B\} \subseteq D(\mathcal{M}) = \{\sigma \in Aut_A B \ : \ \sigma(\mathcal{M}) \subseteq \mathcal{M}\}$. Sejam $\sigma \in D(\mathcal{M})$ e $x \in B$. Então, $x + \mathcal{M} \in \frac{B}{\mathcal{M}} \simeq K$. Como σ é K-linear, segue que $\sigma(x) - x \in \mathcal{M}$. Ou seja, $D(\mathcal{M}) \subseteq T(\mathcal{M})$. Logo, $D(\mathcal{M}) = T(\mathcal{M})$. Pelo Teorema 1.3 de [3], se $T(\mathcal{M}) = D(\mathcal{M}) = \{1\}$ então B/A é galoisiana. Suponha que $\sigma^i(\mathcal{M}) \subseteq \mathcal{M}$ para algum $1 \leqslant i < 4$. Daí, $\sigma^i(X-a) = X+i-a \in \mathcal{M}$. Logo, $i = 2$. Por outro lado, $\sigma^2(Y-b) = Y+1-b \in \mathcal{M}$, o que é um absurdo. Portanto, B/A é uma extensão galoisiana. Observe também que $U(B) = U(K) \subseteq A$. Assim, pelo Lema 8 de [1], B/A não tem elemento primitivo. Note que, o corpo K está contido em qualquer corpo residual de A. Sendo K algebricamente fechado e portanto infinito temos que os corpos residuais de A são todos infinitos. Desta forma, $\frac{B}{\mathcal{M}'B}/\frac{A}{\mathcal{M}'}$ tem elemento primitivo para cada $\mathcal{M}' \in Max(A)$. No entanto, B/A não tem elemento primitivo.

O próximo corolário generaliza o corolário 2.2 de [17].

Corolário 2.4.3. *[26, Teorema 2.4] Sejam R um LG anel e A/R uma extensão fortemente separável de posto constante igual a n. Se para cada $\mathcal{M} \in Max(R)$ temos $\left|\frac{R}{\mathcal{M}}\right| \geq n$ então A/R tem elemento primitivo.*

Demonstração: Seja $\mathcal{M} \in Max(R)$. Da mesma forma que em [17, Corolário 2.2], podemos verificar que a extensão galoisiana $\frac{A}{\mathcal{M}A}/\frac{R}{\mathcal{M}}$ tem elemento primitivo. Conseqüentemente, pela Proposição 2.4.2, A/R tem elemento primitivo. ■

Observação: Fazendo uso da Proposição 2.4.2 podemos estender os seguintes resultados de [17]: Corolário 2.2, Corolário 2.3, Proposição 2.4, Corolário 2.5, Teorema 3.3 e Teorema 3.4. Em [17], estes resultados são demonstrados para extensões galoisianas de um anel semilocal. Usando as mesmas demonstrações de [17] e a Proposição 2.4.2, podemos demonstrá-los para extensões galoisianas de um LG anel. Da mesma forma, o Teorema 2.3, o Corolário 2.9 e o Corolário 2.10 de [15] podem ser estendidos para um LG anel.

Capítulo 3

Polinômios Normais e Polinômios que Geram a Mesma Extensão

No capítulo anterior observamos que a existência de elemento primitivo para uma extensão galoisiana está relacionada com a existência (em número suficiente) de polinômios comaximais que geram a mesma extensão. Neste capítulo, consideraremos polinômios que geram a mesma extensão e que são fatores irredutíveis de um polinômio separável. Conseqüentemente (ver [11, Lema 1.2]), estes polinômios serão dois a dois comaximais. Assim, os resultados obtidos aqui se aplicam ao problema da existência de elemento primitivo. Os resultados deste capítulo generalizam as Proposições 1, 2 e 4 e os Corolários 1 e 3 de [6], não somente obtendo tais resultados para anéis conexos, bem como encontrando outras caracterizações utilizando uma visão categórica dada em [11].

Neste capítulo, R denotará um anel conexo e Ω_R o fecho separável de R. Seguindo [11], denotamos por $C(R)$ o conjunto dos polinômios mônicos e separáveis em $R[X]$.

3.1 Introdução

Nessa seção introduzimos algumas notações que serão utilizadas em todo o capítulo. Da mesma maneira que em [11], dados $f, g \in C(R)$, escreveremos:

$$hom(f,g) = \{t(X) \in R[X] : \ f(t(X)) \in g(X)R[X] \text{ e } \partial t < \partial g\}.$$

Suponha que f e g sejam polinômios irredutíveis em $R[X]$. Além disso, assuma que f e g se escrevem como produto de fatores lineares em $\Omega_R[X]$ da seguinte maneira: $f(X) = (X - a_1)(X - a_2)\dots(X - a_m)$ e $g(X) = (X - b_1)(X - b_2)\dots(X - b_n)$, com

$a_1, \ldots, a_m, b_1, \ldots, b_n \in \Omega_R$. Assuma também que $m \leq n$. Da mesma forma que na demonstração do Lema 2.2.2, temos $\frac{R[X]}{(f)} \simeq R[a_i]$ para todo $1 \leq i \leq m$ e $\frac{R[X]}{(g)} \simeq R[b_j]$ para todo $1 \leq j \leq n$.

Sendo Ω_R uma extensão localmente fortemente separável de R, considere $L \subseteq \Omega_R$ uma extensão fortemente separável de R tal que $\{a_1, a_2, \ldots a_m, b_1, b_2, \ldots b_n\} \subseteq L$. Pelo Teorema 1.1 de [14], podemos mergulhar L numa extensão galoisiana conexa de R. Por isso, assumimos que L/R é galoisiana. Mais ainda, Ω_R/L é uma extensão inteira e $a_i - a_j \in U(\Omega_R)$ $(i \neq j)$, $b_k - b_l \in U(\Omega_R)$ $(k \neq l)$, pois f e g são separáveis (cf.[5, Lema III.4.3]). Assim, $a_i - a_j, b_l - b_k \in U(\Omega_R) \cap L = U(L)$. Pelo Lema 1.7 de [3], $L[X_1, \ldots, X_s]$ é uma extensão galoisiana de $R[X_1, \ldots, X_s]$ com grupo de Galois G igual ao grupo de Galois da extensão L/R, para qualquer $s \in \mathbb{N}$, $s \geq 1$. Além disso, a ação de G se dá sobre os coeficientes de um elemeno de $L[X_1, \ldots, X_s]$. Considere o polinômio,

$$u(X_1, \ldots, X_s) = \prod_{(i_0,\ldots,i_s)\neq(j_0,\ldots,j_s)} [(a_{i_0} - a_{j_0}) + (b_{i_1} - b_{j_1})X_1 + \ldots + (b_{i_s} - b_{j_s})X_s]$$

com $1 \leq i_0, j_0 \leq m$ e $1 \leq i_1, \ldots, i_s, j_1, \ldots, j_s \leq n$. Para cada $\sigma \in G$, temos $\sigma(u) = u$. Portanto, $u \in (L[X_1, \ldots, X_s])^G = R[X_1, \ldots, X_s]$.

Lema 3.1.1. *Com as notações acima, se existem elementos $t_1, \ldots, t_s \in R$ tais que $u(t_1, \ldots, t_s) \in U(R)$ então o polinômio,*

$$H_s(X) = \prod_{i_0,\ldots,i_s} [X - (a_{i_0} + t_1 b_{i_1} + \ldots + t_s b_{i_s})] \in R[X]$$

é separável, onde $1 \leq i_0 \leq m$ e $1 \leq i_1, \ldots, i_s \leq n$.

Demonstração: Note que L é uma extensão galoisiana de R na qual $H_s(X)$ se decompõe em fatores lineares. Mais ainda, as diferenças das raízes de $H_s(X)$ em L são unidades de L. Pelo Teorema 2.2 de [14], $H_s(X)$ é um polinômio separável. ■

Observe que se $u(t_1, \ldots, t_s) \in U(R)$ então $t_k, t_i - t_j \in U(R)$ $(i \neq j)$. De fato, pelo Lema 2.1 de [14], a diferença de duas raízes distintas de H_s é invertível em L. Desta forma, $(a_1 + t_1 b_1 + \ldots + t_k b_1 + \ldots + t_s b_1) - (a_1 + t_1 b_1 + \ldots + t_{k-1} b_1 + t_k b_2 + t_{k+1} b_1 + \ldots + t_s b_1) = t_k(b_1 - b_2) \in U(L)$. Como L/R é uma extensão inteira, temos $U(L) \cap R = U(R)$. Logo, $t_k \in U(L) \cap R = U(R)$. Analogamente, suponha $i < j$ e note que $(a_1 + t_1 b_1 + \ldots + t_i b_1 + \ldots + t_{j-1} b_1 + t_j b_2 + t_{j+1} b_1 + \ldots + t_s b_1) - (a_1 + t_1 b_1 + \ldots + t_{i-1} b_1 + t_i b_2 + t_{i+1} b_1 + \ldots + t_j b_1 + \ldots + t_s b_1) = t_i(b_1 - b_2) + t_j(b_2 - b_1) = (t_i - t_j)(b_1 - b_2) \in U(L)$.

Portanto, $t_i - t_j \in U(R)$.

No restante deste capítulo, usaremos as notações introduzidas nesta seção. Além disso, fixamos $s \in \mathbb{N}$, $s \geq 1$ e assumiremos que existem $t_1, \ldots, t_s \in R$ tais que $u(t_1, \ldots, t_s) \in U(R)$. Assim, pelo lema anterior, o polinômio H_s é separável. Os polinômios $f, g \in R[X]$ serão sempre irredutíveis.

3.2 Polinômios que Geram a Mesma Extensão

Nosso intuíto nesta seção, é caracterizar quando dois polinômios geram a mesma extensão (o que será definido rigorosamente) do anel R. Iniciamos com uma proposição que generaliza o Corolário 3 de [6].

Proposição 3.2.1. *As seguintes afirmações são equivalentes:*

i. Existem $a, b \in \Omega_R$ tais que $f(a) = g(b) = 0$ e $R[a] \subseteq R[b]$.

ii. $hom(f, g) \neq \emptyset$.

iii. O polinômio $H_s(X)$ tem um fator irredutível de grau n em $R[X]$ com uma raiz em Ω_R do tipo $a_i + t_1 b_1 + \ldots + t_s b_1$.

Mais ainda, se $h \in hom(f, g)$ então $\prod_{k=1}^{n} (X - (h(b_k) + t_1 b_k + \ldots + t_s b_k))$ é fator irredutível de $H_s(X)$.

Demonstração: $(i \rightarrow ii)$ Por hipótese, existem $a, b \in \Omega_R$ com $f(a) = g(b) = 0$ e $R[a] \subseteq R[b]$. Desta forma, $a \in R[b]$. Como observamos no início deste capítulo, $R[b] \simeq \frac{R[X]}{(g)}$. Logo, existe $h(X) \in R[X]$ tal que $a = h(b)$ e $\partial h < \partial g$. Portanto, $f(h(b)) = f(a) = 0$. Assim, $f(h(X)) \in (g) = gR[X]$. Conseqüentemente, $h \in hom(f, g)$.

$(ii \rightarrow iii)$ Considere $h \in hom(f, g)$ e tome $\alpha = h(b_1) + t_1 b_1 + \ldots + t_s b_1 \in R[b_1]$. Note que $h(b_1)$ é raiz de f, visto que $f(h(X)) \in (g)$ e $g(b_1) = 0$. Portanto, α é uma raiz de $H_s(X)$. Note também que $b_1, \alpha \in L$. Como L/R é uma extensão fortemente separável e conexa e b_1 e α são raízes de polinômios separáveis sobre R, segue pelo Lema 2.7 de [14], que $R[b_1]$ e $R[\alpha]$ são R-álgebras separáveis. Pela Proposição 1.5 de [14], $R[b_1]$ e $R[\alpha]$ são extensões fortemente separáveis de R. Pelo Corolário 1.3.18 , existem exatamente $rank_R R[\alpha]$ (respec., $rank_R R[b_1]$) homomorfismos de R-álgebras de $R[\alpha]$ para Ω_R (respec., de $R[b_1]$ para Ω_R). Sejam σ, τ dois homomorfismos (de R-álgebras)

distintos de $R[b_1]$ em Ω_R. Então, $\sigma(b_1)$ e $\tau(b_1)$ são raízes distintas de $g(X)$, digamos $\sigma(b_1) = b_j$ e $\tau(b_1) = b_k$, $(j \neq k)$. Logo, $\sigma(\alpha) = h(b_j) + t_1 b_j + \ldots + t_s b_j$ e $\tau(\alpha) = h(b_k) + t_1 b_k \ldots + t_s b_k$. Como H é separável, segue que $\sigma(\alpha) - \tau(\alpha) \in U(L)$. Assim, $\sigma(\alpha) \neq \tau(\alpha)$. Portanto, as restrições de σ e τ para $R[\alpha]$ permanecem homomorfismos distintos. Conseqüentemente, $rank_R R[b_1] \leq rank_R R[\alpha] \leq rank_R R[b_1]$. Pelo Lema 1.1 de [9], $R[\alpha] = R[b_1]$. Note que $R[\alpha] \subseteq \Omega_R$ e $rank_R R[\alpha] = rank_R R[b_1] = \partial g = n$. Pelo Teorema III.3.6 de [5], $R[\alpha] = \Omega_R^H$, onde H é um subgrupo do grupo $\Gamma = Aut_R(\Omega_R)$. Mais ainda, $[\Gamma : H] = n$. Considere $\sigma_1 H, \ldots, \sigma_n H$ as classes laterais distintas de H em Γ. Então, $\{\sigma(\alpha) : \sigma \in \Gamma\} = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$. Por outro lado, $\{\sigma_j(b_1) : j = 1, \ldots, n\} = \{b_1, \ldots, b_n\}$. Portanto, $\{\sigma_j(\alpha) : j = 1, \ldots, n\} = \{h(b_k) + t_1 b_k + \ldots + t_s b_k : k = 1, \ldots, n\}$. Assim,

$$t(X) = \prod_{k=1}^{n} (X - (h(b_k) + t_1 b_k + \ldots + t_s b_k))$$

é um fator de H_s. Observe também, que o polinômio acima é invariante pela ação de cada $\sigma \in \Gamma$. Pelo Teorema 1.3.21, $\Omega_R^\Gamma = R$. Desta forma, o polinômio $t(X)$ é um fator de H_s e pertence a $R[X]$. Pelo Lema 1.2 de [11], o polinômio $t(X)$ é separável, visto que H_s é separável. Mais ainda, Γ age transitivamente nas raízes de $t(X)$. Portanto, pelo Lema 1.5 de [11], $t(X)$ é um polinômio irredutível em $R[X]$.

$(iii \to i)$ Tome $v(X)$ um fator irredutível de grau n de $H_s(X)$ e $\alpha = a_i + t_1 b_1 + \ldots + t_s b_1$ uma raiz de v. Suponha que $a_i \notin R[b_1]$. Observe que a função multiplicação $\mu : R[a_i] \otimes_R R[b_1] \longrightarrow R[a_i, b_1]$ é um homomorfismo sobrejetor de R-álgebras. Pela Proposição 1.3.13, como $R[a_i]$ e $R[b_1]$ são R-álgebras separáveis, temos que $R[a_i] \otimes_R R[b_1]$ é uma R-álgebra separável. Segue então, da Proposição 1.3.4, que $R[a_i, b_1]$ é uma R-álgebra separável. Pelo Lema 1.1 de [9], $rank_R R[a_i, b_1] > rank_R R[b_1]$. Observe que $R \subseteq R[\alpha] \subseteq R[a_i, b_1] \subseteq L$. Sendo que L/R é uma extensão fortemente separável e $R[\alpha]$ e $R[a_i, b_1]$ são R-álgebras separáveis, temos pela Proposição 1.5 de [14] que $R[\alpha]$ e $R[a_i, b_1]$ são extensões fortemente separáveis de R. Sejam σ, τ homomorfismos distintos de $R[a_i, b_1]$ para Ω_R. Então, $\sigma(a_i) \neq \tau(a_i)$ ou $\sigma(b_1) \neq \tau(b_1)$. Portanto, $\sigma(\alpha) - \tau(\alpha) \in U(L)$. Usando a mesma argumentação feita em $(ii \to iii)$ via o posto destas extensões, concluímos que $R[\alpha] = R[a_i, b_1]$. Daí, $n = rank_R R[\alpha] = rank_R R[a_i, b_1] > rank_R R[b_1] = n$, o que é um absurdo. Conseqüentemente, $a_i \in R[b_1]$. Logo, $R[a_i] \subseteq R[b_1]$.

Observe que a última afirmação da proposição já foi provada em $(ii) \to (iii)$. ■

Definição 3.2.2. *Dados $f, g \in C(R)$ polinômios irredutíveis, $\partial f = \partial g$, diremos que f e g geram a mesma extensão de R se $\frac{R[X]}{(f)} \simeq \frac{R[X]}{(g)}$ como R-álgebras, ou equivalentemente, se existem $a, b \in \Omega_R$ tais que $f(a) = g(b) = 0$ e $R[a] = R[b]$.*

Fazendo $m = \partial f = n = \partial g$ na proposição acima, obtemos um corolário que generaliza a Proposição 2 de [6].

Corolário 3.2.3. *As seguintes afirmações são equivalentes:*

i. f, g *geram a mesma extensão de* R.

ii. *Existem* $a, b \in \Omega_R$ *tais que* $f(a) = g(b) = 0$ *e* $R[a] = R[b]$.

iii. $hom(f, g) \neq \emptyset$.

iv. *O polinômio* $G_s(X) = \prod_{1 \leq i_o, \ldots, i_s \leq n} [X - (a_{i_o} + t_1 b_{i_1} + \ldots + t_s b_{i_s})] \in R[X]$ *tem um fator irredutível de grau* n *com uma raiz do tipo* $a_i + t_1 b_1 + \ldots + t_s b_1$.

Mais ainda, se $h \in hom(f, g)$ *então* $\prod_{k=1}^{n} (X - (h(b_k) + t_1 b_k + \ldots t_s b_k))$ *é um fator irredutível de* $G(X)$ *de grau* n.

Agora reproduziremos, para a comodidade do leitor, o Teorema 2.3 de [11]. Este teorema introduz uma operação no conjunto dos polinômios mônicos. Denote por $M(R)$ o conjunto dos polinômios mônicos em $R[X]$. Portanto, $M(R)$ é a categoria cujos objetos são os polinômios mônicos. Mais ainda, dados dois objetos $f, g \in M(R)$ um morfismo entre f e g é um elemento em $hom(f, g)$ e a operação introduzida a seguir será a operação entre morfismos desta categoria. Observe que o conjunto dos polinômios separáveis em $R[X]$, o qual denotamos por $C(R)$, é uma subcategoria de $M(R)$.

Teorema 3.2.4. *Sejam $f, g, h \in M(R)$, $k \in hom(f, g)$ e $l \in hom(g, h)$. Então existe um único $t \in hom(f, h)$ e um único $w \in h(X)R[X]$ com $k(l(X)) = t(X) + w(X)$. Denotaremos t por $l \circ k$.*

No restante deste capítulo, "$\circ$" não denotará a composição de funções, mas sim a operação introduzida no teorema acima. No corolário seguinte reobtemos o Teorema 2.6 de [11].

Corolário 3.2.5. *Sejam $f, g \in C(R)$ polinômios irredutíveis.*

i. Se $hom(f,g) \neq \emptyset$ então ∂f divide ∂g.

ii. Se $hom(f,g) \neq \emptyset$ e $\partial f = \partial g$ então para cada $k \in hom(f,g)$ existe $t \in hom(g,f)$ tal que $k \circ t = X \in hom(g,g)$ e $t \circ k = X \in hom(f,f)$.

Demonstração: (i) Pela Proposição 3.2.1, existem $a, b \in \Omega_R$ tais que $f(a) = g(b) = 0$ e $R[a] \subseteq R[b]$. Assim, $\partial f = rank_R R[a]$ divide $rank_R R[b] = \partial g$.

(ii) Sejam $k \in hom(f,g)$ e $b \in \Omega_R$ tal que $g(b) = 0$. Então, $a = k(b)$ é raiz de f. Como $\partial f = \partial g$, segue do Lema 1.1 de [9] que $R[a] = R[b]$. Tome $t(X) \in R[X]$, $\partial t < \partial f$ com $t(a) = b$. Logo, $g(t(a)) = g(b) = 0$. Daí, $t \in hom(g,f)$. Também, $b = t(a) = t(k(b))$. Desta forma, b é raiz de $t(k(X)) - X$, ou seja, $t(k(X)) - X \in (g)$. Assim, $t(k(X))) = q(X)g(X) + X$ para algum $q(X) \in R[X]$. Pelo teorema acima, temos $k \circ t = X$. De forma análoga, obtém-se $t \circ k = X$. ■

O corolário acima nos assegura que se $\partial f = \partial g$ então $hom(f,g) \neq \emptyset$ se e somente se $hom(g,f) \neq \emptyset$. Portanto, podemos incluir no Corolário 3.2.3 uma (v) equivalência: (v) $hom(g,f) \neq \emptyset$.

3.3 Polinômios Normais

Em [6] defini-se polinômio normal sobre um corpo da seguinte maneira: sejam K um corpo, $f(X) \in K[X]$ um polinômio irredutível e a uma raiz de f no fecho algébrico de K. Se $K[a]/K$ é uma extensão normal de corpos então f é dito normal. Por outro lado, em [11] diz-se que um polinômio mônico, separável e irredutível $f \in R[X]$ (onde R é um anel conexo) é normal se $\#hom(f,f) = n$. A definição de polinômio normal sobre um anel conexo dada aqui, estende naturalmente a definição de [6]. Mostraremos que tal definição é equivalente a definição de [11]. No restante desta seção encontramos condições necessárias e suficientes para que dois polinômios gerem a mesma extensão e (ou) sejam normais. Obtemos também outras caracterizações de polinômio normal.

Definição 3.3.1. *Sejam $f \in C(R)$ um polinômio irredutível e $a \in \Omega_R$ uma raiz de f. Dizemos que f é normal se a extensão $R[a]/R$ é normal, isto é, $R[a]^G = R$ com $G = Aut_R(R[a])$.*

Lema 3.3.2. *Seja $f \in C(R)$ um polinômio irredutível de grau n. As seguintes afirmações são equivalentes:*

i. f *é normal.*

ii. $\#hom(f,f) = \partial f = n$.

iii. Se $a \in \Omega_R$ *é uma raiz de* f *então todas as raízes de* f *em* Ω_R *estão em* $R[a]$.

iv. Para cada $a \in \Omega_R$ *tal que* $f(a) = 0$ *temos que* $R[a]$ *é uma extensão galoisiana de* R *com grupo* $H = Aut_R R[a]$.

Demonstração: $(i \rightarrow ii)$ Seja $a \in \Omega_R$ com $f(a) = 0$. Por hipótese, $R[a]/R$ é normal. Pelo Lema 2.7 de [14], $R[a]/R$ é separável. Portanto, $R[a]/R$ é galoisiana. Considere $H = \{\sigma_1, \ldots, \sigma_n\}$ o grupo de Galois de $R[a]$ sobre R. Para cada $1 \leq j \leq n$, $\sigma_j(a)$ é uma raiz de f em $R[a]$. Portanto, $\sigma_j(a) = h_j(a)$, com $h_j(X) \in R[X]$ e $\partial h_j < \partial f = n$. Note que se $i \neq j$ então $\sigma_i(a) \neq \sigma_j(a)$. Logo, para $(i \neq j)$ temos que $h_i(X) \neq h_j(X)$. Desta forma, $f(h_j(a)) = f(\sigma_j(a)) = 0$. Daí, $f(h_j(X)) \in (f)$. Conseqüentemente, $h_1, \ldots, h_n \in hom(f,f)$. Se $u \in hom(f,f)$ então $u(a)$ é uma raiz de f e $u(a) \in R[a]$. Pelo Lema 2.1 de [14], $\{\text{raízes de } f \text{ em } R[a]\} = \{\sigma_j(a) : j = 1 \ldots n\}$. Assim, $u(a) = \sigma_j(a)$ para algum $j \in \{1, \ldots, n\}$. Ou seja, $u(a) = h_j(a)$. Pelo Corolário 3.2.5, existe $u^{-1} \in hom(f,f)$ tal que $u \circ u^{-1} = X$. Pelo Teorema 3.2.4, $a = u^{-1}(u(a)) = u^{-1}(h_j(a))$. Então, $u^{-1}(h_j(X)) - X \in (f)$. Portanto, $h_j \circ u^{-1} = X$. Conseqüentemente, $u = h_j$ em $hom(f,f)$. Logo, $hom(f,f) = \{h_1, \ldots, h_n\}$.

$(ii \rightarrow iii)$ Seja $a \in \Omega_R$ tal que $f(a) = 0$. Suponha que $b \in \Omega_R$ é tal que $f(b) = 0$ e $b \notin R[a]$. Por hipótese, $hom(f,f) = \{h_1, \ldots, h_n\}$. Assim, $h_j(a)$ são raízes de f e estão em $R[a]$. Como $b \notin R[a]$, temos que $b \neq h_j(a)$ para qualquer $j = 1, \ldots, n$. Portanto, f possui no mínimo $(n+1)$ raízes em $R[a,b]$. Observe que $\mu : R[a] \otimes_R R[b] \longrightarrow R[a,b]$ é um homomorfismo sobrejetor de R-álgebras. Mas, $R[a]$ e $R[b]$ são R-álgebras separáveis. Pela Proposição 1.3.13, $R[a] \otimes_R R[b]$ é uma R-álgebra separável. Sendo μ sobrejetor, segue da Proposição 1.3.4, que $R[a,b]$ é uma R-álgebra separável. Então, pelo Lema 2.1 de [14], f possui no máximo n raízes em $R[a,b]$. Assim, temos uma contradição. Daí, $b \in R[a]$.

$(iii \rightarrow i)$ Seja $a \in \Omega_R$ tal que $f(a) = 0$. Por hipótese, se $f(X) = (X - a_1) \ldots (X - a_n)$ em $\Omega_R[X]$ então $a_i \in R[a]$ para todo $1 \leq i \leq n$. Para cada j, defina $\sigma_j : R[a] \longrightarrow R[a]$ por $\sigma_j(a) = a_j$. Note que pela hipótese, σ_j está bem definido. Mas ainda, σ_j é um automorfismo, pois $\frac{R[X]}{(f)} \simeq R[a]$ e $\frac{R[X]}{(f)} \simeq R[a_j]$. Assim, $\#Aut_R(R[a]) \geq n$. Pelo Corolário 2.2 de [9], $\#Aut_R(R[a]) \leq rank_R(R[a]) = n$. Logo, $\#Aut_R(R[a]) = rank_R(R[a])$. Novamente pelo Corolário 2.4 de [9], $R[a]^H = R$ onde $H = Aut_R(R[a])$. Portanto, $R[a]/R$ é normal.

$(i \to iv)$ Como vimos em $(i \to ii)$, para cada $a \in \Omega_R$ tal que $f(a) = 0$ temos que $R[a]$ é uma extensão galoisiana de R. Pelo Teorema 3.5 de [3], o grupo de Galois da extensão $R[a]/R$ é $H = Aut_R R[a]$.

$(iv \to i)$ Imediato.

■

Exemplos:
(1) Vamos verificar que cada polinômio $f \in C(R)$ de grau 2 é normal. Dado $f = X^2 + aX + b \in R[X]$, considere $f_1 = X$ e $f_2 = -X - a$. Note que $f(f_i(X)) = f(X)$ para $i = 1, 2$. Portanto, $hom(f, f) = \{f_1, f_2\}$. Conseqüentemente, f é normal em $R[X]$.
(2) Seja $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$. Então, é fácil verificar que $hom(f, f) = \{f_1 = X, f_2 = X^2, f_3 = X^3, f_4 = -X^3 - X^2 - X - 1\}$. Assim, f é normal em $\mathbb{Q}[X]$.

Corolário 3.3.3. *Se $f \in C(R)$ é um polinômio irredutível e normal de grau n então $hom(f, f)$ é um grupo de ordem n.*

Demonstração: Sejam $u, v \in hom(f, f)$. Pelo Teorema 3.2.4, $u \circ v \in hom(f, f)$. Pelo Corolário 3.2.5, cada elemento de $hom(f, f)$ tem um inverso em $hom(f, f)$. Note que $e = e(X) = X \in hom(f, f)$ é a identidade, isto é, para qualquer $h \in hom(f, f)$ temos $h \circ e = e \circ h = h$. Pelo lema acima, temos que $\#hom(f, f) = n$. Assim, $hom(f, f)$ é um grupo de ordem n. ■

Agora vamos verificar que se $f \in C(R)$ é um polinômio irredutível e normal então $hom(f, f) \simeq Aut_R\left(\frac{R[X]}{(f)}\right)$. Portanto, a menos de isomorfismo, o grupo de Galois da extensão $\frac{R[X]}{(f)}/R$ é $hom(f, f)$. Para tanto, usaremos o lema a seguir.

Lema 3.3.4. *Sejam $f \in C(R)$ um polinômio irredutível de grau n, $h \in hom(f, f)$ e $x = X + (f)$. Então:*

i. $\Psi : \frac{R[X]}{(f)} \longrightarrow \frac{R[X]}{(f)}$ *definida por* $\Psi(x) = h(x)$, *é um elemento de* $Aut_R\left(\frac{R[X]}{(f)}\right)$.

ii. Se $\Psi \in Aut_R\left(\frac{R[X]}{(f)}\right)$ *e* $\Psi(x) = h(x)$ *então* $h \in hom(f, f)$.

Demonstração: (i) Tome $u(X), v(X) \in R[X]$ polinômios tais que $u - v \in (f)$, ou seja, $u - v = f.g$ para algum $g \in R[X]$. Note que $f(h(X)) = f(X).l(X)$ para algum $l \in R[X]$. Assim, $(u - v)(h(X)) = (f.g)(h(X)) = f(h(X)).g(h(X)) = f(X).l(X).g(h(X)) \in (f)$. Portanto, $u(h(x)) = v(h(x))$. Desta forma, Ψ está

bem definida. Claramente, Ψ (estendida por linearidade) é um homomorfismo de R-álgebras. Suponha que $\Psi(u(x)) = 0$. Então, $u(h(x)) = 0$, ou seja, $u(h(X)) = f(X).v(X)$ para algum $v(X) \in R[X]$. Seja $t \in hom(f,f)$ tal que $t \circ h = X \in hom(f,f)$. Daí, $h(t(X)) - X \in (f)$. Logo, $h(t(a_i)) = a_i$ para qualquer $1 \leq i \leq n$. Conseqüentemente, $u(a_i) = u(h(t(a_i))) = f(t(a_i)).v(t(a_i)) = 0$, pois $t \in hom(f,f)$. Portanto, $u(x) = 0$ e Ψ é injetora. Observe que, $\frac{R[X]}{(f)} \simeq \Psi\left(\frac{R[X]}{(f)}\right) \subseteq \frac{R[X]}{(f)}$. Pelo Lema 1.1 de [9], temos $\Psi\left(\frac{R[X]}{(f)}\right) = \frac{R[X]}{(f)}$. Então, Ψ é também sobrejetora e o resultado segue.

(ii) Como $\{1, x, \ldots, x^{n-1}\}$ é uma R-base de $\frac{R[X]}{(f)}$ temos que $\partial(h) < n = \partial(f)$. Além disso, $0 = \Psi(0) = \Psi(f(x)) = f(h(x))$. Desta forma, $f(h(X)) \in (f)$. Logo, $h(X) \in hom(f,f)$. ■

Corolário 3.3.5. *Seja $f \in C(R)$ um polinômio irredutível, normal e de grau n e suponha que $hom(f,f) = \{f_1, \ldots, f_n\}$. Então $\frac{R[X]}{(f)}/R$ é uma extensão galoisiana com grupo $H = Aut_R\left(\frac{R[X]}{(f)}\right) = \{\sigma_j : j = 1, \ldots, n\}$, onde $\sigma_j(x) = f_j(x)$ e $x = X + (f)$.*

Demonstração: Como vimos no Lema 3.3.2, $\frac{R[X]}{(f)}/R$ é uma extensão galoisiana com grupo $H = Aut_R\left(\frac{R[X]}{(f)}\right)$. Pelo Lema 3.3.4, para cada $1 \leq j \leq n$, definindo $\sigma_j(x) = f_j(x)$ temos que $\sigma_j \in H$. É fácil ver também que se $i \neq j$ então $\sigma_i \neq \sigma_j$. Sendo que $\#H = \partial(f) = n$, segue que $H = \{\sigma_j : j = 1, \ldots, n\}$. ■

Corolário 3.3.6. *Se $f \in C(R)$ é um polinômio irredutível e normal então os grupos $hom(f,f)$ e $H = Aut_R\left(\frac{R[X]}{(f)}\right)$ são isomorfos.*

Demonstração: Suponha que $hom(f,f) = \{f_1, \ldots, f_n\}$. Pelo Corolário 3.3.5, $\sigma_j : \frac{R[X]}{(f)} \longrightarrow \frac{R[X]}{(f)}$ dada por $\sigma_j(x) = f_j(x)$, onde $x = X + (f)$, é um elemento de H. Defina $\phi : hom(f,f) \longrightarrow H$ por $\phi(f_j) = \sigma_j$. Claramente ϕ é uma bijeção. Além disso, dados $f_i, f_j \in hom(f,f)$ temos $\phi(f_i \circ f_j)(x) = f_j(f_i(x)) = \phi(f_i)(f_j(x)) = \phi(f_i)(\phi(f_j)(x))$. Portanto, $\phi(f_i \circ f_j) = \phi(f_i) \circ \phi(f_j)$, onde $\circ$ do lado esquerdo denota a operação entre os morfismos da categoria $M(R)$ e $\circ$ do lado direito a composição usual de funções. Conseqüentemente, ϕ é um isomorfismo de grupos. ■

Usaremos o Lema 3.3.2 para provar o próximo resultado, o qual generaliza o Corolário 1 de [6].

Proposição 3.3.7. *Sejam $f, g \in C(R)$ polinômios irredutíveis tais que $f(X) = (X - a_1)\ldots(X - a_n)$ e $g(X) = (X - b_1)\ldots(X - b_n)$ em $\Omega_R[X]$. As seguintes afirmações são equivalentes:*

i. f, g *geram a mesma extensão de* R *e são normais.*

ii. $\#hom(f,g) = n$.

iii. $\#hom(g,f) = n$.

iv. $G_s(X) = \prod_{1 \leq i_o, \ldots, i_s \leq n} [X - (a_{i_o} + t_1 b_{i_1} + \ldots + t_s b_{i_s})]$ *tem* n^s *fatores irredutíveis de grau* n*, sendo que* n *destes fatores possuem uma raiz do tipo* $a_i + t_1 b_1 + \ldots + t_s b_1$.

Mais ainda, se $hom(g,f) = \{h_1, \ldots, h_n\}$ *então*

$$\prod_{k=1}^{n} (X - (a_k + t_1 h_{i_1}(a_k) + \ldots + t_s h_{i_s}(a_k)))$$

é fator irredutível de $G(X)$ *para cada escolha* $(i_1, \ldots, i_s)$ *com* $i_j \in \{1, \ldots, n\}$.

Demonstração: $(i \to ii)$ Pelo Corolário 3.2.3, sabemos que existe $h \in hom(f,g)$. Pelo Lema 3.3.2, $hom(g,g) = \{g_1, \ldots, g_n\}$. Segue do Teorema 3.2.4, que $g_j \circ h \in hom(f,g)$ para todo $1 \leq j \leq n$. Seja $u \in hom(f,g)$. Pelo Corolário 3.2.5 existe $t \in hom(g,f)$ com $t \circ h = X \in hom(f,f)$. Note que pela definição da operação entre os morfismos da categoria $M(R)$ temos $u \circ t \in hom(g,g)$. Daí, $u \circ t = g_j$, para algum $j \in \{1, \ldots, n\}$. Logo, $u = u \circ X = u \circ t \circ h = g_j \circ h$, ou seja, $u = g_j \circ h$. Assim, $hom(f,g) = \{g_j \circ h : j = 1, \ldots, n\}$.

$(ii \to iii)$ Imediato do Corolário 3.2.5, parte (ii).

$(iii \to iv)$ Suponha que $hom(g,f) = \{h_1, \ldots, h_n\}$ e tome $\alpha(i_1, \ldots, i_s) = a_1 + t_1 h_{i_1}(a_1) + \ldots + t_s h_{i_s}(a_1) \in R[a_1]$. Observe que $h_{i_j}(a_1) \in \{b_1, \ldots, b_n\}$. Raciocinando como na Proposição 3.2.1 $(ii \to iii)$, obtemos $R[\alpha(i_1, \ldots, i_s)] = R[a_1]$ para cada escolha $(i_1, \ldots, i_s)$. Portanto,

$$\prod_{k=1}^{n} [X - (a_k + t_1 h_{i_1}(a_k) + \ldots + t_s h_{i_s}(a_k))]$$

é um fator irredutível de G_s de grau n. Observe que para cada $1 \leq j \leq n$, os fatores obtidos de G_s a partir da escolha $\alpha(j, \ldots, j)$ possuem uma raiz do tipo desejada.

$(iv \to i)$ Pelo Corolário 3.2.3 e pela hipótese, f e g geram a mesma extensão de R. Falta verificar que f e g são normais. Suponha que f não é normal. Pelo Lema 3.3.2, $a_i \notin R[a_1]$ para algum i. Como f e g geram a mesma extensão, $R[a_1] = R[b_k]$

para algum $k \in \{1, \ldots, n\}$. Tome $\alpha = a_i + t_1 b_k + \ldots + t_s b_k \in R[a_i, b_k]$. Usando novamente a argumentação feita na Proposição 3.2.1, obtemos $R[\alpha] = R[a_i, b_k]$ e $rank_R R[a_i, b_k] > rank_R R[b_k] = n$. Portanto, G_s possui um fator irredutível de grau maior que n, contrariando a hipótese. Logo, f é normal. De forma análoga verifica-se que g é normal. ■

Note que na demonstração de $(iv \rightarrow i)$ usamos a hipótese de G possuir fatores irredutíveis com raízes do tipo $a_i + t_1 b_1 + \ldots + t_s b_1$ somente para garantir que f e g geram a mesma extensão de R. Sendo assim, no caso em que $g = f$ podemos excluir essa hipótese. Então temos um corolário, o qual generaliza a Proposição 1 de [6].

Corolário 3.3.8. *Seja $f \in C(R)$ um polinômio irredutível, $f(X) = (X - a_1) \ldots (X - a_n)$ em $\Omega_R[X]$. As seguintes afirmações são equivalentes:*

i. f é normal.

ii. $\#hom(f, f) = n$.

iii. $F_s(X) = \prod_{1 \leq i_o, \ldots, i_s \leq n} [X - (a_{i_o} + t_1 a_{i_1} + \ldots + t_s a_{i_s})]$ é o produto de n^s fatores irredutíveis de grau n em $R[X]$.

Mais ainda, se $hom(f, f) = \{f_1, \ldots, f_n\}$ então os fatores irredutíveis de $F_s(X)$ são da forma :

$$\prod_{k=1}^{n} [X - (a_k + t_1 f_{i_1}(a_k) + \ldots + t_s f_{i_s}(a_k))] .$$

Observação: Observando a demonstração da Proposição 3.3.7 concluímos que f e cada fator do polinômio F_s geram a mesma extensão de R. Mais ainda, como F_s é separável, segue do Lema 1.2 de [11] que os ideais gerados pelos seus fatores são dois a dois comaximais. Portanto, a decomposição de F_s produz n^s polinômios mônicos, separáveis e irredutíveis que geram a mesma extensão de f e cujos respectivos ideais gerados são dois a dois comaximais. Então podemos utilizar os fatores irredutíveis de F_s no problema da existência do elemento primitivo, como veremos no próximo teorema.

Suponha que $S = S_1 \oplus \ldots \oplus S_r / R$ é uma extensão galoisiana de posto m e que uma de suas componentes conexas, digamos S_i, possui elemento primitivo. Tome $f \in R[X]$ um polinômio separável e irredutível tal que $S_i = \frac{R[X]}{(f)}$ e $\partial(f) = n$. Dado $s \in \mathbb{N}$, assuma que os polinômios $u(X_1, \ldots, X_s)$ e F_s são construídos a partir das raízes de f em Ω_R. Com essas notações temos o seguinte teorema.

Teorema 3.3.9. *Se para $s \in \mathbb{N}$ tal que $s \geq log_n r$ existem $t_1, \ldots, t_s \in U(R)$ tal que $u(t_1, \ldots, t_s) \in U(R)$ então S/R tem elemento primitivo.*

Demonstração: Pela observação anterior, $\#I_R(S_i) \geq n^s$. Mas por hipótese, $s \geq log_n r$. Portanto, $n^s \geq r$. Assim, $\#I_R(S_i) \geq r$. Pelo Teorema 2.3.2, S/R tem elemento primitivo. ■

3.4 Critérios Matriciais

Nessa seção, daremos critérios envolvendo o determinante de matrizes construídas a partir das raízes dos polinômios, para decidir quando estes são normais e (ou) geram a mesma extensão de R.

Iniciamos introduzindo algumas notações necessárias. Sejam $f, g \in C(R)$ polinômios irredutíveis com $f(X) = (X - a_1) \ldots (X - a_n)$ e $g(X) = (X - b_1) \ldots (X - b_n)$ em $\Omega_R[X]$. Denotamos por

$$D = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix}.$$

Para cada $\sigma \in S_n$ (grupo de permutações), D_k^σ denotará o determinante obtido de D trocando a k-ésima linha por $(b_{\sigma(1)}, \ldots, b_{\sigma(n)})$.

A próxima proposição generaliza a Proposição 4 de [6].

Proposição 3.4.1. *Com a notação acima, as seguintes afirmações são equivalentes:*

i. f e g geram a mesma extensão de R.

ii. $hom(g, f) \neq \emptyset$.

iii. Existe $\sigma \in S_n$ tal que $D_k^\sigma = \lambda_k D$, com $\lambda_k \in R$ para todo $1 \leq k \leq n$.

Nesse caso, $h(X) = r_1 + \ldots + r_n X^{n-1} \in hom(g, f)$ e $h(a_i) = b_{\sigma(i)}$ se e somente se $D_k^\sigma = r_k D$ para todo $1 \leq k \leq n$.

Demonstração: $(i \rightarrow ii)$ Segue do Corolário 3.2.3 e do Corolário 3.2.5.

$(ii \rightarrow iii)$ Se $h \in hom(g, f)$ então $g(h(a_i)) = 0$. Assuma que $h(X) = r_1 + \ldots + r_n X^{n-1} \in R[X]$. Considere uma extensão fortemente separável L de R tal que

$\{a_1, \ldots, a_n, b_1, \ldots, b_n\} \subseteq L$. Pelo Lema 2.1 de [14], $b_1, \ldots, b_n$ são todas as raízes de g em L. Note que $h(a_i)$ é uma raiz de g que está em L, pois $h(a_i) \in R[a_i] \subseteq L$. Portanto, $h(a_i) = b_{j_i}$. Note também que $h(a_i) \neq h(a_j)$ se $i \neq j$. De fato, suponha que para $i \neq j$ temos $h(a_i) = h(a_j)$. Pelo Corolário 3.2.5, existe $t \in hom(f, g)$ tal que $h \circ t = X \in hom(f, f)$. Pela definição da operação $\circ$, temos que $t(h(X)) = f(X)q(X) + X$ para algum $q(X) \in R[X]$. Então, $a_i = t(h(a_i)) = t(h(a_j)) = a_j$. Mas isto é um absurdo. Portanto, $h(a_i) \neq h(a_j)$. Desta forma, se tomarmos σ tal que $\sigma(i) = j_i$, temos que $\sigma \in S_n$. Assim,

$$D_k^\sigma = \begin{vmatrix} 1 & 1 & 1 & \cdots & \cdots & 1 & 1 \\ a_1 & a_2 & a_3 & \cdots & \cdots & a_{n-1} & a_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1^{k-2} & a_2^{k-2} & a_3^{k-2} & \cdots & \cdots & a_{n-1}^{k-2} & a_n^{k-2} \\ h(a_1) & h(a_2) & h(a_3) & \cdots & \cdots & h(a_{n-1}) & h(a_n) \\ a_1^k & a_2^k & a_3^k & \cdots & \cdots & a_{n-1}^k & a_n^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \cdots & \cdots & a_{n-1}^{n-1} & a_n^{n-1} \end{vmatrix}.$$

Conseqüentemente, $D_k^\sigma = r_k D$ para todo $1 \leq k \leq n$.

$(iii \rightarrow i)$ Tome $\sigma \in S_n$ e $\lambda_1, \ldots, \lambda_n \in R$ tais que $D_k^\sigma = \lambda_k D$. Observe que $D = \prod_{i>j}(a_i - a_j)$. Como f é um polinômio separável, segue do Lema 2.1 de [14], que $a_i - a_j \in U(\Omega_R)$. Logo, $D \in U(\Omega_R)$. Assim, $v_1 = (1, \ldots, 1)$, $v_2 = (a_1, \ldots, a_n), \ldots, v_n = (a_1^{n-1}, \ldots, a_n^{n-1})$ é uma Ω_R-base de $\Omega_R^n = \Omega_R \times \ldots \times \Omega_R$ (n-vezes). Portanto, $(b_{\sigma(1)}, \ldots, b_{\sigma(n)}) = s_1 v_1 + \ldots + s_n v_n$, $s_i \in \Omega_R$. De forma análoga ao que foi feito acima, temos $D_k^\sigma = s_k D$. Assim, $s_k = D_k^\sigma D^{-1} = \lambda_k \in R$. Logo, $b_{\sigma(1)} \in R[a_1]$ e então $R[b_{\sigma(1)}] = R[a_1]$. Desta forma, f e g geram a mesma extensão. Observe também que se $h(X) = \lambda_1 + \ldots + \lambda_n X^{n-1}$ então $h(a_i) = b_{\sigma(i)}$ e $h \in hom(g, f)$.

Note que a última afirmação da proposição foi verificada nas demonstrações de $(ii \rightarrow iii)$ e $(iii \rightarrow i)$. ■

Agora gostaríamos de ter um critério matricial, não somente para decidir se f e g geram a mesma extensão, mas também para dizer se f e g são normais. Tal critério é dado na próxima proposição.

Proposição 3.4.2. *As seguintes afirmações são equivalentes:*

i. f e g geram a mesma extensão de R e são normais.

ii. $\#hom(g,f) = n$.

iii. Existem exatamente n *permutações* $\sigma_1, \ldots, \sigma_n \in S_n$ *tais que* $D_k^{\sigma_j} = \lambda_{kj} D$, $\lambda_{kj} \in R$, *para todo* $1 \leq k, j \leq n$.

Nesse caso, $hom(g,f) = \{h_1, \ldots, h_n\}$, $h_j(X) = r_{1j} + r_{2j}X + \ldots + r_{nj}X^{n-1} \in R[X]$ *e* $h_j(a_i) = b_{\sigma_j(i)}$ *se e somente se* $D_k^{\sigma_j} = r_{kj}D$, *para todo* $1 \leq k, j \leq n$.

Demonstração: $(i \leftrightarrow ii)$ Segue da Proposição 3.3.7.

$(ii \rightarrow iii)$ Suponha que $hom(g,f) = \{h_1, \ldots, h_n\}$. Para cada j, temos $g(h_j(X)) \in (f)$. Mais ainda, $h_j(a_i)$ é raiz de g, para todo $1 \leq i \leq n$. Suponha que $h_j(a_i) = b_{j_i}$, $1 \leq j_i \leq n$, e defina $\sigma_j(i) = j_i$. Da mesma forma que na proposição anterior, temos que $h_j(a_m) \neq h_j(a_l)$ se $m \neq l$. Portanto, $\sigma_j \in S_n$. Note também que $h_j(a_i) \neq h_l(a_i)$ $(j \neq l)$. De fato, suponha que para $j \neq l$ temos $h_j(a_i) = h_l(a_i)$. Pelo Corolário 3.2.5, existe $t \in hom(f,g)$ tal que $h_j \circ t = X \in hom(f,f)$ e $t \circ h_j = X \in hom(g,g)$. Então, $t(h_j(X)) = f(X)q(X) + X$ para algum $q(X) \in R[X]$. Conseqüentemente, $a_i = t(h_j(a_i)) = t(h_l(a_i))$. Assim, $t(h_l(X)) - X \in (f)$. Pela definição da operação $\circ$, temos $h_l \circ t = X \in hom(f,f)$. Portanto, $h_l = h_l \circ X = h_l \circ t \circ h_j = X \circ h_j = h_j$. Mas isto é um absurdo. Daí, temos que $h_j(a_i) \neq h_l(a_i)$ se $j \neq l$. Assim, $\sigma_j \neq \sigma_l$ para $j \neq l$. Como na Proposição 3.4.1, se $h_j(X) = r_{1j} + r_{2j}X + \ldots + r_{nj}X^{n-1} \in R[X]$ então $D_k^{\sigma_j} = r_{kj}D$. Falta apenas verificar que existem exatamente n permutações satisfazendo (iii). Suponha que existe $\tau \in S_n$ tal que $D_k^{\tau} = r_k D$ e $\tau \notin \{\sigma_1, \ldots, \sigma_n\}$. Então, é fácil ver que $h(X) = r_1 + \ldots + r_n X^{n-1} \in hom(g,f)$ e $h \notin \{h_1, \ldots, h_n\}$. Mas isso contradiz a nossa hipótese. Portanto, existem exatamente n permutações satisfazendo (iii).

$(iii \rightarrow i)$ Sejam $\sigma_1, \ldots, \sigma_n \in S_n$ tais que $D_k^{\sigma_j} = \lambda_{kj} D$, $\lambda_{kj} \in R$ para todo $1 \leq k, j \leq n$. Note que como D é uma unidade em Ω_R, existem $s_{kj} \in \Omega_R$, $k, j = 1, \ldots, n$, tais que $(b_{\sigma_j(1)}, \ldots, b_{\sigma_j(n)}) = s_{1j}v_1 + \ldots + s_{nj}v_n$, para todo $1 \leq j \leq n$. Daí, $D_k^{\sigma_j} D^{-1} = s_{kj} = \lambda_{kj}$. Tome $h_j(X) = \lambda_{1j} + \lambda_{2j}X + \ldots + \lambda_{nj}X^{n-1} \in R[X]$ para todo $1 \leq j \leq n$. Então, $h_j(a_i) = b_{\sigma_j(i)}$. Conseqüentemente, $g(h_j(a_1)) = g(b_{\sigma_j(1)}) = 0$. Mas, $\frac{R[X]}{(f)} \simeq R[a_1]$. Assim, $h_j(X) \in hom(g,f)$ para todo $1 \leq j \leq n$. Usando o fato das permutações serem distintas, verifica-se imediatamente que os polinômios $h_j's$ são distintos. Portanto, $\#hom(g,f) \geq n$. Seja $u(X) = r_1 + r_2X + \ldots + r_nX^{n-1} \in hom(g,f)$. Então, $u(a_i) = b_{j_i}$. Definindo $\sigma(i) = j_i$ temos que $\sigma \in S_n$ e $D_k^{\sigma} = r_k D$. Pela hipótese, $\sigma = \sigma_j$ para algum $j \in \{1, \ldots, n\}$. Então, $r_k D = \lambda_{kj} D$ para todo $1 \leq k \leq n$. Logo, $r_k = \lambda_{kj}$ para todo $1 \leq k \leq n$. Desta forma, $u(X) = h_j(X)$ e

$hom(g, f) = \{h_1, \ldots, h_n\}$. Pela Proposição 3.3.7, f e g geram a mesma extensão e são normais. ■

Dado $\sigma \in S_n$ denote por T_k^σ o determinante obtido de D trocando a k-ésima linha por $(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$. O próximo resultado é conseqüência imediata da proposição anterior.

Corolário 3.4.3. *As seguintes afirmações são equivalentes:*

i. f *é normal.*

ii. $\#hom(f, f) = \partial f = n$.

iii. Existem exatamente n *permutações* $\sigma_1, \ldots, \sigma_n \in S_n$ *tais que* $T_k^{\sigma_j} = \lambda_{kj} D$, $\lambda_{kj} \in R$, *para todo* $1 \leq k, j \leq n$.

Nesse caso, $hom(f, f) = \{h_1, \ldots, h_n\}$, $h_j(X) = r_{1j} + r_{2j}X + \ldots + r_{nj}X^{n-1} \in R[X]$ *e* $h_j(a_i) = a_{\sigma_j(i)}$ *se e somente se* $T_k^{\sigma_j} = r_{kj} D$, *para todo* $1 \leq k, j \leq n$.

Para finalizar, o próximo resultado nos diz que $hom(f, f)$ é um subgrupo do grupo S_n, quando f é normal e $\partial f = n$. Na verdade, podemos associar a cada $f_j \in hom(f, f)$ uma permutação das raízes de f.

Corolário 3.4.4. *Seja* $f(X)$ *um polinômio normal. Então existe* $H \subseteq S_n$ *um subgrupo de ordem* n *e um anti-isomorfismo de grupos de* $hom(f, f)$ *para* H.

Demonstração: Pelo Corolário 3.4.3, existem $\sigma_1, \ldots, \sigma_n \in S_n$. Vamos verificar que $H = \{\sigma_1, \ldots, \sigma_n\}$ é um grupo. Conforme a demonstração da Proposição 3.4.2, se $hom(f, f) = \{f_1, \ldots, f_n\}$ e $f_j(a_i) = a_{j_i}$ então $\sigma_j(i) = j_i$. Tome σ_j e σ_k em H e os respectivos f_j e f_k em $hom(f, f)$. Suponha que $f_j(a_i) = a_{j_i}$ e $f_k(a_{j_i}) = a_{k_{j_i}}$. Como $hom(f, f)$ é um grupo temos que $f_j \circ f_k \in hom(f, f)$. Além disso, pela operação do grupo $hom(f, f)$ temos $f_j \circ f_k(a_i) = a_{k_{j_i}}$. Assim, $\sigma_k \circ \sigma_j$ é o elemento de H obtido de $f_j \circ f_k$. Claramente $1 \in H$, pois $X \in hom(f, f)$. Logo, H é um subgrupo de S_n e $\Psi : hom(f, f) \longrightarrow H$ dada por $\Psi(f_j) = \sigma_j$ é um anti-isomorfismo de grupos. ■

Observe que no Corolário acima $\sigma_k \circ \sigma_j$ significa a composição de funções enquanto $f_j \circ f_k$ é a operação introduzida entre os morfismos da categoria $M(-)$.

Capítulo 4

Uma Forma Fraca do Teorema do Elemento Primitivo

Como vimos no Capítulo 2, em geral, uma extensão fortemente separável (em particular, uma extensão galoisiana) de um anel comutativo não possui elemento primitivo. Também vimos que, nos casos possíveis, a existência de elemento primitivo só é assegurada mediante alguma restrição sobre o anel de base.

Em [23], T. McKenzie apresenta uma forma fraca do teorema do elemento primitivo para anéis locais (Teorema 1.1 de [23]). O resultado de McKenzie afirma que se $(R, \mathcal{M})$ é um anel local e S/R é uma extensão fortemente separável e conexa então existem $\alpha \in \Omega_R$ e $f(X) \in R[X]$ um polinômio mônico, separável e irredutível tais que $f(\alpha) = 0$ e $S \subseteq R[\alpha]$.

Sejam R um anel conexo e Ω_R o seu fecho separável. Se para cada extensão fortemente separável e conexa S de R existem $\alpha \in \Omega_R$ e $f(X) \in R[X]$ um polinômio mônico, separável e irredutível tais que $f(\alpha) = 0$ e $S \subseteq R[\alpha]$, diremos que R é um anel que satisfaz a forma fraca do teorema do elemento primitivo e escreveremos: R satisfaz a (f.f.e.p.).

Na primeira seção deste capítulo, introduzimos a noção de anel localmente uniforme e provamos que os anéis conexos cujo quociente pelo radical (radical de Jacobson) são von Neumann regulares e localmente uniformes satisfazem a (f.f.e.p.). Em particular, para cada anel semilocal, o quociente pelo radical de Jacobson é von Neumann regular e localmente uniforme. No entanto, no caso semilocal obtemos informações adicionais e por isso apresentamos uma demonstração independente para este caso (seção 4.2).

4.1 Anéis Localmente Uniformes

Em [4] defini-se anel uniforme da seguinte maneira. Sejam R um anel e $X = Spec(B(R))$ o espectro booleano de R. Dizemos que R é uniforme se para cada $x \in X$ existe uma coleção de isomorfismos $\Phi_y : R_y \longrightarrow R_x$, onde y varia em X, tal que se $F \subseteq R$ é um subconjunto finito então existe uma vizinhança V de x com $\Phi_y(a_y) = a_x$ para todo $a \in F$ e para todo $y \in V$.

Como veremos no exemplo abaixo, em geral, para um anel semilocal o anel quociente $\frac{R}{J(R)}$ não é uniforme. Nosso objetivo é provar a forma fraca do teorema do elemento primitivo para uma classe de anéis que contenha os anéis semilocais. Para tanto, introduzimos a seguinte definição.

Definição 4.1.1. *Sejam R um anel e $X = Spec(B(R))$ o espectro booleano de R. Dizemos que R é localmente uniforme se para cada $x \in X$ e para cada $F \subseteq R$ subconjunto finito existem uma vizinhança V=V(x,F) de x e uma coleção de isomorfismos $\Phi_y : R_y \longrightarrow R_x$, onde y varia em V, tal que $\Phi_y(a_y) = a_x$ para todo $a \in F$ e para todo $y \in V$.*

Lembremos que um anel comutativo R é dito von Neumann regular se para cada $r \in R$ existe $s \in R$ tal que $r = r^2s$. É sabido que R é von Neumann regular se e somente se cada elemento de R é produto de um idempotente de R por uma unidade de R. Conseqüentemente, se R é um anel comutativo conexo e von Neumann regular então R é um corpo. Note que se R é um anel semilocal então $\frac{R}{J(R)}$ é um produto cartesiano finito de corpos. Logo, $\frac{R}{J(R)}$ é von Neumann regular.

Exemplo: Claramente todo anel uniforme é localmente uniforme. No entanto a recíproca não é verdadeira. De fato, considere um anel semilocal R e assuma que $Max(R) = \{\mathcal{M}_1, \ldots, \mathcal{M}_t\}$ e que os seus corpos residuais não são todos isomorfos. Então, $\frac{R}{J(R)}$ é um anel semilocal com $Max\left(\frac{R}{J(R)}\right) = \left\{\frac{\mathcal{M}_1}{J(R)}, \ldots, \frac{\mathcal{M}_t}{J(R)}\right\}$. Note que $B\left(\frac{R}{J(R)}\right)$ é um anel finito. Assim, $X = Spec\left(B\left(\frac{R}{J(R)}\right)\right)$ é finito. Na verdade pode-se verificar que $\#X = t$. Para cada $x \in X$ considere a vizinhança $V_x = \{x\}$ e o isomorfismo $\Phi_x : \left(\frac{R}{J(R)}\right)_x \longrightarrow \left(\frac{R}{J(R)}\right)_x$ como sendo a identidade de $\left(\frac{R}{J(R)}\right)_x$. Então, $\frac{R}{J(R)}$ é localmente uniforme. Por outro lado, para cada $x \in X$ temos que $\left(\frac{R}{J(R)}\right)_x$ é von Neumann regular e conexo. Portanto, $\left(\frac{R}{J(R)}\right)_x$ é um corpo. Mais ainda, $\left(\frac{R}{J(R)}\right)_x = \frac{\frac{R}{J(R)}}{I(x)}$, ou seja, $I(x) = \frac{\mathcal{M}}{J(R)}$ para algum $\mathcal{M} \in Max(R)$. Logo, $\left(\frac{R}{J(R)}\right)_x \simeq \frac{R}{\mathcal{M}}$. Como os corpos residuais não são todos isomorfos, temos que $\frac{R}{J(R)}$ não é uniforme.

A próxima observação é importante e será usada frequentemente no restante do trabalho, inclusive no próximo teorema.

Observação 4.1.2. *Sejam S/R uma extensão fortemente separável e conexa e $\mathcal{M} \in Max(R)$. O conjunto dos ideais maximais de S que estão sobre $\mathcal{M}$ (isto é, o conjunto dos ideais maximais de S que interceptados com R são iguais a $\mathcal{M}$) é igual ao conjunto dos ideais maximais de S que não interceptam $R - \mathcal{M}$. Mas este por sua vez, está em bijeção com o conjunto dos ideais maximais de $S_{\mathcal{M}}$ (o localizado segundo o sistema multiplicativo $R-\mathcal{M}$). Pela Proposição 2.3 de [14], $S_{\mathcal{M}}$ é uma $R_{\mathcal{M}}$-álgebra fortemente separável. Pelo corolário do Lema 2 de [28], temos que $S_{\mathcal{M}}$ é um anel semilocal. Portanto, o número de ideais maximais de S que estão sobre $\mathcal{M}$ é finito.*

Apresentaremos agora a forma fraca do teorema do elemento primitivo para anéis conexos cujo quociente pelo seu radical é von Neumann regular e localmente uniforme.

Teorema 4.1.3. *Se S/R é uma extensão fortemente separável e conexa e $\frac{R}{J(R)}$ é um anel von Neumann regular e localmente uniforme então existem $\beta \in \Omega_R$ e $u \in R[X]$ um polinômio mônico, separável e irredutível tais que $u(\beta) = 0$ e $S \subseteq R[\beta]$.*

Demonstração: Sejam $\overline{R} = \frac{R}{J(R)}$, $\overline{S} = \frac{S}{J(R)S} = \frac{S}{J(S)}$ e $X = X(\overline{R})$ o espectro booleano de $\overline{R}$. Note que $\overline{R}_x = \frac{\overline{R}}{I(x)}$ é von Neumann regular e conexo, para cada $x \in X(\overline{R})$. Portanto, $\overline{R}_x$ é um corpo. Pelo Teorema 1.1 de [14], cada extensão fortemente separável e conexa imerge numa extensão galoisiana e conexa. Então, podemos assumir que S/R é galoisiana. Suponha que $rank_R S = n$ e que $Y = \{x \in X \ : \ |\overline{R}_x| < \infty\}$. A demonstração será feita em 02 casos.

<u>1º caso</u>: $Y = \emptyset$

Nesse caso, $|\overline{R}_x| = \infty$ para todo $x \in X$. É bem conhecido que cada extensão separável e finita de um corpo infinito tem elemento primitivo. Então, $\overline{S}_x/\overline{R}_x$ tem elemento primitivo para cada $x \in X$. Pelo Teorema 2.1.2, $\overline{S}/\overline{R}$ tem elemento primitivo, ou seja, $\overline{S} = \overline{R}[\overline{\beta}]$, onde $\overline{\beta} = \beta + J(S)$. Daí, $S = R[\beta] + J(S) \subseteq R[\beta] + \mathcal{M}S \subseteq S$, para cada $\mathcal{M} \in Max(R)$. Pelo lema de Nakayama generalizado ([5, Corolário I.1.8]), $S = R[\beta]$. Pela Proposição 2.2.3, existe $u(X) \in R[X]$ um polinômio mônico, separável e irredutível tal que $u(\beta) = 0$.

<u>2º caso</u>: $Y \neq \emptyset$

Nesse caso, considere $q = min\{|\overline{R}_x| \ : \ x \in Y\}$. Como já observamos, $\overline{R}_z = \frac{\overline{R}}{I(z)}$ é um corpo para cada $z \in X$. Assim, $I(z)$ é um ideal maximal de $\overline{R}$. Mas, $Max(\overline{R}) =$

$\left\{\frac{\mathcal{M}}{J(R)} \ : \ \mathcal{M} \in Max(R)\right\}$. Desta forma, para cada $z \in X$ existe $\mathcal{M} \in Max(R)$ tal que $I(z) = \frac{\mathcal{M}}{J(R)}$. Tome $p \in \mathbb{N}$ um número primo tal que $\frac{q^p - q}{p} \geqslant n$ e p não divide n. Dado $y \in Y$ considere $f_y(X) = (a_0)_y + (a_1)_y X + \ldots + (a_{p-1})_y X^{p-1} + X^p \in \overline{R}_y[X]$ um polinômio separável e irredutível e $f(X) = a_0 + a_1 X + \ldots + a_{p-1}X^{p-1} + X^p \in \overline{R}[X]$. Note que o polinômio $f_y(X)$ existe, pois $\overline{R}_y$ é um corpo finito. Por hipótese, existe uma vizinhança $N(f_1)$ de y e isomorfismos $\Phi_z : \overline{R}_z \longrightarrow \overline{R}_y$ tal que $\Phi_z((a_j)_z) = (a_j)_y$ para todo $0 \leq j \leq p-1$ e para todo $z \in N(f_1)$. Como f_y é separável sobre $\overline{R}_y$, segue do Corolário 1.3 e do Teorema 2.3 de [25] que $\delta(f_y) = \delta(f)_y$ é invertível em $\overline{R}_y$. Assim, existe $\lambda \in \overline{R}$ tal que $(\delta(f)\lambda)_y = 1_y$. Pela Proposição 1.2.8, existe uma vizinhança $N(f_2)$ de y tal que $(\delta(f)\lambda)_x = 1_x$, para qualquer $x \in N(f_2)$. Mais ainda, $(\delta(f)\lambda)f_2 = f_2$. Tomando a intersecção das vizinhanças $N(f_1)$ e $N(f_2)$, podemos considerar um idempotente $e(y) = f_1 f_2$ em $B(\overline{R})$, uma vizinhança $N(e(y))$ de y tal que $(\delta(f)\lambda)_z = 1_z$ para todo $z \in N(e(y))$, $(\delta(f)\lambda)e(y) = e(y)$ e isomorfismos $\Phi_z : \overline{R}_z \longrightarrow \overline{R}_y$ com $\Phi_z((a_j)_z) = (a_j)_y$ para todo $0 \leq j \leq p-1$ e para todo $z \in N(e(y))$. Observe também que $f_z(X) = (a_0)_z + (a_1)_z X + \ldots + (a_{p-1})_z X^{p-1} + X^p \in \overline{R}_z[X]$ é irredutível (pois Φ_z é um isomorfismo) para todo $z \in N(e(y))$ e que $f(X)e(y)$ é irredutível em $\overline{R}[X]e(y)$. De fato, se existem $u(X), v(X) \in \overline{R}[X]$ polinômios mônicos de grau maior ou igual a 1 tais que $f(X)e(y) = u(X)e(y)v(X)e(y)$ então $f_y(X) = u_y(X)v_y(X)$ contrariando a irredutibilidade de $f_y(X)$.

Dado $x \in X - Y$, considere um polinômio separável $g_x(X) = (b_0)_x + (b_1)_x X + \ldots + (b_{p-1})_x X^{p-1} + X^p \in \overline{R}_x[X]$ e $g(X) = b_0 + b_1 X + \ldots + b_{p-1}X^{p-1} + X^p \in \overline{R}[X]$. Note que o polinômio $g_x(X)$ existe pois o corpo $\overline{R}_x$ é infinito. Usando a separabilidade de $g_x(X)$, o Corolário 1.3, o Teorema 2.3 de [25] e a Proposição 1.2.8, obtemos uma vizinhança $N(e(x))$ de x tal que $g_z(X)$ é separável em $\overline{R}_z[X]$ para todo $z \in N(e(x))$ e $g(X)e(x)$ é separável em $\overline{R}[X]e(x)$.

Usando o argumento de compacidade usual, existem idempotentes $e_1, \ldots, e_r \in B(\overline{R})$ e polinômios mônicos $f_1, \ldots, f_r \in \overline{R}[X]$ de grau p tais que: $e_1 + \ldots + e_r = 1$, $e_i e_j = 0$ se $(i \neq j)$, $f_i e_i$ é separável para todo $1 \leq i \leq r$ e $f_i e_i$ é irredutível se $N(e_i)$ é vizinhança de algum $y \in Y$. Tome $h = f_1 e_1 + \ldots + f_r e_r \in \overline{R}[X]$. Note que h é um polinômio mônico de grau p. Vamos verificar que h é separável em $\overline{R}[X]$. De fato, pelo corolário 1.3 de [25], $\delta(he_i) = \delta(h)e_i$ e $\delta(f_i e_i) = \delta(f_i)e_i$ para todo $1 \leq i \leq r$. Logo, $\delta(h) = \delta(h)e_1 + \ldots + \delta(h)e_r = \delta(he_1) + \ldots + \delta(he_r) = \delta(f_1)e_1 + \ldots + \delta(f_r)e_r$. Como $\delta(f_j)e_j \in U(\overline{R}e_j)$ e os idempotentes são dois a dois ortogonais temos que $\delta(h) \in U(\overline{R})$. Pelo Teorema 2.3 de [25], $h \in \overline{R}[X]$ é um polinômio separável. Seja $t(X) \in R[X]$ um polinômio mônico de grau p tal que

$\overline{t} = h \ (mod\, J(R))$. Pelo Corolário 1.3 de [25], $\delta(\overline{t}) = \overline{\delta(t)} = \delta(h) \in U(\overline{R})$. Daí, $\delta(t) \in U(R)$ e conseqüentemente $t(X)$ é um polinômio separável em $R[X]$.

Agora provaremos que $t(X)$ é um polinômio irredutível em $S[X]$. Suponha que $t(X) = r_0 + r_1X + \ldots + r_{p-1}X^{p-1} + X^p \in R[X]$ e seja $y \in Y$. Então, $\overline{t}_y(X) = (\overline{r}_0)_y + (\overline{r}_1)_yX + \ldots + (\overline{r}_{p-1})_yX^{p-1} + X^p \in \overline{R}_y[X]$. Por outro lado, $\overline{t}_y(X) = (f_i)_y(X)$ para algum $i \in \{1, \ldots, r\}$ e $y \in N(e_i)$. Como $y \in Y$ temos que $(f_i)_y(X)$ é irredutível em $\overline{R}_y[X]$. Suponha que $I(y) = \frac{\mathcal{M}}{J(R)}$ e que $\mathcal{P}_1, \ldots, \mathcal{P}_s$ são todos os ideais maximais de S que estão sobre $\mathcal{M}$ (ver Observação 4.1.2). Então temos $\overline{R}_y \simeq \frac{R}{\mathcal{M}}$, sendo o isomorfismo dado por $\Psi(\overline{r}_y) = r + \mathcal{M}$. Note que o polinômio $\Psi(\overline{t}_y(X)) = (r_0 + \mathcal{M}) + (r_1 + \mathcal{M})X + \ldots + (r_{p-1} + \mathcal{M})X^{p-1} + X^p \in \frac{R}{\mathcal{M}}[X]$ é irredutível. Mas p não divide n e então p não divide $\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]$. Desta forma, o polinômio $(r_0 + \mathcal{P}_1) + (r_1 + \mathcal{P}_1)X + \ldots + (r_{p-1} + \mathcal{P}_1)X^{p-1} + X^p \in \frac{S}{\mathcal{P}_1}[X]$ é irredutível, ou seja, $\overline{t}$ visto em $\frac{S}{\mathcal{P}_1}[X]$ é um polinômio irredutível. Portanto, $t(X) \in S[X]$ é irredutível. Já vimos que $t(X)$ é separável em $R[X]$. Daí, como $R \simeq R.1 \subseteq S$ temos que $t(X)$ é separável em $S[X]$. Tome $T = \frac{S[X]}{(t(X))}$. Pela escolha de $t(X)$ temos que T/S é uma extensão fortemente separável e conexa (cf.Lema 2.2.2). Pela transitividade da separabilidade e pela Proposição 1.5 de [14], temos que T/R é uma extensão fortemente separável e conexa.

Vamos verificar que $\overline{T}_x/\overline{R}_x$ tem elemento primitivo para cada $x \in X$, onde $\overline{T} = \frac{T}{J(T)} = \frac{T}{J(R)T}$. Claramente, se $x \in X - Y$ então $\overline{T}_x/\overline{R}_x$ tem elemento primitivo. Seja $y \in Y$ e suponha que $I(y) = \frac{\mathcal{M}}{J(R)}$ e que $\mathcal{P}_1, \ldots, \mathcal{P}_s$ são todos os ideais maximais de S que estão sobre $\mathcal{M}$ (ver Observação 4.1.2). De forma análoga ao que fizemos acima, prova-se que $\overline{t}$ visto em $\frac{S}{\mathcal{P}_j}[X]$ é irredutível para cada $1 \leq j \leq s$. Pelo Teorema 3.5 de [21], T possui apenas um ideal maximal $\mathcal{P}'_j$ sobre $\mathcal{P}_j$ e $\left[\frac{T}{\mathcal{P}'_j} : \frac{S}{\mathcal{P}_j}\right] = p$. Portanto, $\left[\frac{T}{\mathcal{P}'_j} : \frac{R}{\mathcal{M}}\right] = p\left[\frac{S}{\mathcal{P}_j} : \frac{R}{\mathcal{M}}\right] = p\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]$, pois $\frac{S}{\mathcal{P}_j} \simeq \frac{S}{\mathcal{P}_1}$ já que S/R é galoisiana. Denote por $N_q(n)$ o número de polinômios mônicos e irredutíveis de grau n sobre o corpo finito com q elementos. É fácil verificar que a função $\frac{X^p - X}{p}$ é crescente em $[1, \infty)$. Pelo Teorema 3.25 de [18], temos $N_q(p) = \frac{q^p - q}{p}$. Portanto, se $|\overline{R}_y| = q_y$ então $N_{q_y}(p) = \frac{q_y^p - q_y}{p} \geq \frac{q^p - q}{p} = N_q(p)$, pois $q = min\{|\overline{R}_x| \ : \ x \in Y\}$. Se $\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right] = 1$ então $N_{q_y}\left(p\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]\right) = N_{q_y}(p) \geq N_q(p) \geq n$. Se $\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right] \geq 2$ então pelo Lema 1.2 de [15] temos $N_{q_y}\left(p\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]\right) \geq N_{q_y}(p)N_{q_y}\left(\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]\right) \geq N_{q_y}(p) \geq N_q(p) \geq n$. Portanto, $N_{q_y}\left(p\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]\right) \geq n \geq s$. Assim, existem $h_1, \ldots, h_s$ polinômios mônicos separáveis e irredutíveis de grau $p\left[\frac{S}{\mathcal{P}_1} : \frac{R}{\mathcal{M}}\right]$ em $\frac{R}{\mathcal{M}}[X]$. Pelo Teorema 2.1 de [21],

$\mathcal{M}T = \bigcap_{j=1}^{s} \mathcal{P}'_j$. Usando o teorema do resto Chinês temos, $\frac{T}{\mathcal{M}T} = \frac{T}{\mathcal{P}'_1} \oplus \ldots \oplus \frac{T}{\mathcal{P}'_s}$. Mais ainda, $\frac{T}{\mathcal{P}'_j} \simeq \frac{\frac{R}{\mathcal{M}}[X]}{(h_j)}$ para cada $1 \leq j \leq s$. Novamente pelo teorema Chinês, $\frac{T}{\mathcal{M}T} \simeq \frac{\frac{R}{\mathcal{M}}[X]}{(h_1 \ldots h_s)}$. Portanto, $\frac{T}{\mathcal{M}T}/\frac{R}{\mathcal{M}}$ tem elemento primitivo. Agora observe que $\overline{T}_y = \frac{\overline{T}}{I(y)\overline{T}} = \frac{\frac{T}{J(T)}}{\frac{\mathcal{M}T}{J(T)}} \simeq \frac{T}{\mathcal{M}T}$. Desta forma, $\overline{T}_y/\overline{R}_y$ tem elemento primitivo. Como y é um elemento arbitrário de Y segue que $\overline{T}_x/\overline{R}_x$ tem elemento primitivo para todo $x \in X$. Da mesma forma que no primeiro caso, T/R tem elemento primitivo, ou seja, existem $\beta \in T$ e $u(X) \in R[X]$ um polinômio irredutível tais que $u(\beta) = 0$ e $S \subseteq R[\beta]$. ■

Os próximos corolários generalizam os corolários 1.2 e 1.4 de [23] e suas demonstrações são idênticas as dadas em [23]. No entanto, as repetiremos aqui para a comodidade do leitor.

Antes porém, reproduziremos a definição de fecho polinomial que foi dada originalmente por F. DeMeyer em [4]. Em [4], prova-se também a existência e unicidade, a menos de isomorfismo, do fecho polinomial para um anel conexo.

Definição 4.1.4. *Sejam R um anel conexo e Γ uma extensão localmente fortemente separável e conexa de R. Dizemos que Γ é um fecho polinomial se:*

i. qualquer subconjunto finito de Γ está contido em uma extensão de R da forma $R[\alpha_1, \ldots, \alpha_n] \subseteq \Gamma$, sendo que α_i é raiz de um polinômio separável sobre $R[\alpha_1, \ldots, \alpha_{i-1}]$;

ii. cada polinômio separável sobre R se decompõe em fatores lineares em $\Gamma[X]$.

Corolário 4.1.5. *Se R é um anel conexo tal que $\frac{R}{J(R)}$ é um anel von Neumann regular e localmente uniforme então o fecho separável de R e o fecho polinomial de R coincidem.*

Demonstração: Pelo Teorema III.4.4 de [5], cada polinômio separável e mônico em $R[X]$ é um produto de fatores lineares em $\Omega_R[X]$. Sejam $\alpha_1, \ldots, \alpha_n \in \Omega_R$. Então, existe uma extensão S/R fortemente separável e conexa tal que $\alpha_1, \ldots, \alpha_n \in S$. Pelo teorema anterior, existe $\alpha \in \Omega_R$ raiz de um polinômio mônico, separável e irredutível sobre R tal que $S \subseteq R[\alpha]$. Portanto, Ω_R é um fecho polinomial de R. Pela unicidade, o fecho separável de R e o fecho polinomial de R são iguais. ■

Corolário 4.1.6. *Sejam R um anel conexo tal que $\frac{R}{J(R)}$ é um anel von Neumann regular e localmente uniforme e $T \subseteq \Omega_R$ um subanel tal que $R \subseteq T$. Então $\Omega_R = \Omega_T$.*

Demonstração: Precisamos provar que Ω_R é uma extensão localmente fortemente separável de T. Sejam $\alpha_1, \ldots, \alpha_n \in \Omega_R$. Pelo Teorema anterior, existem $\alpha \in \Omega_R$ e $f(X) \in R[X]$ um polinômio mônico, separável e irredutível tal que $f(\alpha) = 0$ e $\alpha_1, \ldots, \alpha_n \in R[\alpha]$. Temos também, $\frac{T[X]}{(f)} \simeq T \otimes_R \frac{R[X]}{(f)}$. Como $\frac{R[X]}{(f)}$ é uma R-álgebra separável, segue que $\frac{T[X]}{(f)}$ é um T-álgebra separável. Assim, $T[\alpha]$ é uma T-álgebra fortemente separável e $T[\alpha] \subseteq \Omega_R$. Mas, $R[\alpha] \subseteq T[\alpha]$. Daí, $\alpha_1, \ldots, \alpha_n \in T[\alpha]$. Portanto, Ω_R é uma extensão fortemente separável de T. Sendo que Ω_R é separavelmente fechado, temos $\Omega_R = \Omega_T$. ■

Como vimos no exemplo no início desta seção, se R é um anel semilocal então $\frac{R}{J(R)}$ é um anel localmente uniforme. O próximo exemplo mostra que existem anéis conexos com infinitos ideais maximais e tais que o quociente pelo radical são anéis von Neumann regular e localmente uniformes. Portanto, o conjunto dos anéis semilocais e conexos está contido e é diferente do conjunto dos anéis conexos cujo quociente pelo radical é von Neumann regular e localmente uniforme. Este exemplo foi sugerido pelo professor Yves Lequain, ao qual somos gratos.

Exemplo: Sejam $p \in \mathbb{Z}$ um número primo positivo e $R = \mathbb{Z}_{(p)}$ o localizado de $\mathbb{Z}$ segundo o sistema multiplicativo $S = \mathbb{Z} - p\mathbb{Z}$. Segundo um resultado da teoria de números devido a H. Hasse ([12]) , o qual pode ser visto em [7, pg.185], existe uma extensão quadrática K_1 de $\mathbb{Q}$ tal que $p\mathbb{O}_1 = q_1 q_2$, onde $\mathbb{O}_1$ é o fecho inteiro de $\mathbb{Z}_{(p)}$ em K_1 e q_1 e q_2 são os únicos ideais maximais de $\mathbb{O}_1$ que estão sobre $p\mathbb{Z}_{(p)}$. Novamente, pelo mesmo teorema, existe uma extensão quadrática K_2 de K_1 tal que $q_1\mathbb{O}_2 = q_{11}q_{12}$ e $q_2\mathbb{O}_2 = q_{21}q_{22}$ onde $\mathbb{O}_2$ é o fecho inteiro de $\mathbb{O}_1$ em K_2, q_{11} e q_{12} são os únicos ideais maximais de $\mathbb{O}_2$ que estão sobre q_1 e q_{21} e q_{22} são os únicos ideais maximais de $\mathbb{O}_2$ que estão sobre q_2. Da mesma forma, considere uma extensão quadrática K_3 de K_2 na qual cada ideal maximal q_{ij} decompõe-se em dois ideais maximais. Continue este processo um número infinito de vezes e considere $L = \bigcup_{j=1}^{\infty} K_j$ e $\mathbb{O}$ o fecho inteiro de $\mathbb{Z}_{(p)}$ em L. Claramente temos $\mathbb{O}_1 \subseteq \mathbb{O}_2 \subseteq \ldots \subseteq \mathbb{O}$. Como em cada etapa cada ideal maximal se decompõe em outros dois ideais maximais e como $\mathbb{O}/\mathbb{Z}_{(p)}$ é uma extensão inteira, segue que $\#Max(\mathbb{O}) = \infty$. Além disso, cada ideal maximal de $\mathbb{O}$ está sobre $p\mathbb{Z}_{(p)}$. Portanto, $p\mathbb{O} \subseteq J(\mathbb{O})$ e daí, $J(\mathbb{O}) \neq 0$. Lembre que a dimensão de Krull de um anel R é dada por: $dim(R) = sup\{ht(\mathcal{P}) : \mathcal{P} \in Spec(R)\}$, onde $ht(\mathcal{P})$ é o comprimento da maior cadeia de ideais primos do tipo $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \ldots \subsetneq \mathcal{P}_n = \mathcal{P}$. Observe que como $\mathbb{Z}_{(p)}$ é um anel local então $dim(\mathbb{Z}_{(p)}) = ht(p\mathbb{Z}_{(p)})$. Mais ainda, $\mathbb{Z}_{(p)}$ é um domínio de ideais principais. Portanto, $dim(\mathbb{Z}_{(p)}) = 1$. Sendo $\mathbb{O}/\mathbb{Z}_{(p)}$

uma extensão inteira de anéis, temos que $dim(\mathbb{O}) = 1$. Assim, $dim\left(\frac{\mathbb{O}}{p\mathbb{O}}\right) = 0$. Pelo Lema 1 de [10], $\frac{\frac{\mathbb{O}}{p\mathbb{O}}}{J\left(\frac{\mathbb{O}}{p\mathbb{O}}\right)}$ é von Neumann regular. Mas, $\frac{\frac{\mathbb{O}}{p\mathbb{O}}}{J\left(\frac{\mathbb{O}}{p\mathbb{O}}\right)} = \frac{\frac{\mathbb{O}}{p\mathbb{O}}}{\frac{J(\mathbb{O})}{p\mathbb{O}}} \simeq \frac{\mathbb{O}}{J(\mathbb{O})}$. Conseqüentemente, $\mathbb{O}$ é um anel conexo com infinitos ideais maximais e $\frac{\mathbb{O}}{J(\mathbb{O})}$ é von Neumann regular. Note que $\mathbb{O} = \bigcup_{j=1}^{\infty} \mathbb{O}_j$. Mais ainda, $\frac{\mathbb{O}_j}{\mathcal{P}} \simeq \mathbb{Z}_p$ para todo $j \in \mathbb{N}$ e para todo $\mathcal{P} \in Spec(\mathbb{O}_j)$. Seja $\mathcal{P} \in Spec(\mathbb{O})$ e $x \in \frac{\mathbb{O}}{\mathcal{P}}$. Então, $x = a + \mathcal{P}$ com $a \in \mathbb{O}$. Logo, $a \in \mathbb{O}_j$ para algum $j \in \mathbb{N}$. Então, $x \in \frac{\mathbb{O}_j}{\mathcal{P} \cap \mathbb{O}_j} \simeq \mathbb{Z}_p$. Desta forma, $\frac{\mathbb{O}}{\mathcal{P}} \simeq \mathbb{Z}_p$ para todo $\mathcal{P} \in Spec(\mathbb{O})$. Considere $R = \frac{\mathbb{O}}{J(\mathbb{O})}$ e $X = Spec(B(R))$. Neste caso, note que $R_z \simeq \mathbb{Z}_p$ para cada $z \in X$. Assim, $R_z = \{0_z, 1_z, \ldots, (p-1)_z\}$. Tome $x \in X$ e $F \subseteq R$ finito, digamos $F = \{a_1, \ldots, a_n\}$. Para cada $i \in \{0, \ldots, p-1\}$, considere $I_i = \{1 \leq j \leq n \ : \ (a_j)_x = i_x\}$. Note que a união dos conjuntos $I_i's$ é igual ao conjunto $\{1, \ldots, n\}$ e que I_i pode ser vazio. Se $I_i \neq \emptyset$, para cada $j \in I_i$, tome uma vizinhança V_j de x tal que $(a_j)_y = i_y$ para todo $y \in V_j$. Seja $V = \bigcap_{j=1}^{n} V_j$. Note que V é uma vizinhança de x e que $(a_j)_y = (a_j)_x$ para todo $1 \leq j \leq n$ e para todo $y \in V$. Então, para cada $y \in V$, a função $\Phi_y : R_y \longrightarrow R_x$ dada por $\Phi_y(i_y) = i_x$ é um isomorfismo e satisfaz a condição exigida na definição de anel localmente uniforme. Portanto, R é um anel localmente uniforme.

4.2 Caso Semilocal

Nessa seção apresentamos uma demonstração independente da forma fraca do teorema do elemento primitivo para o caso semilocal. Além disso, obtemos informações relacionadas com o posto das extensões.

Teorema 4.2.1. *Se S/R é uma extensão fortemente separável e conexa e R é um anel semilocal então existem $\alpha \in \Omega_R$ e $u(X) \in R[X]$ um polinômio separável e irredutível tais que $u(\alpha) = 0$ e $S \subseteq R[\alpha] = T$. Mais ainda, podemos escolher um número primo ímpar p tal que $rank_R T = p^i \cdot rank_R S$, onde $i = 0$ ou $i = 1$.*

Demonstração: Por simplicidade, vamos supor que $Max(R) = \{\mathcal{M}_1, \mathcal{M}_2\}$. Para um número finito qualquer de ideais maximais, segue-se raciocínio análogo ao feito aqui. A demonstração será dividida em 03 casos.

<u>1º caso</u>: $\left|\frac{R}{\mathcal{M}_i}\right| = \infty, \ \ i = 1, 2.$

Neste caso, pelo Corolário 2.4.3, S/R tem elemento primitivo. Portanto, existe $\alpha \in S$ tal que $S = R[\alpha]$. Conseqüentemente, pela Proposição 2.2.3, existe $u(X) \in R[X]$ um polinômio mônico, separável e irredutível tal que $u(\alpha) = 0$.

<u>2^o caso</u>: $\left|\frac{R}{\mathcal{M}_i}\right| < \infty, \ \ i = 1, 2.$

Suponha que os ideais maximais de S que estão sobre $\mathcal{M}_1$ sejam $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ e os ideais maximais de S que estão sobre m_2 sejam $\mathcal{P}_1, \ldots, \mathcal{P}_m$ (ver Observação 4.1.2). Os números primos positivos constituem um subconjunto infinito dos números naturais. Então, tome $p \in \mathbb{N}$ um número primo suficientemente grande ($p > 2$) tal que p não divide $\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]$ para todo $1 \leq j \leq n$, p não divide $\left[\frac{S}{\mathcal{P}_i} : \frac{R}{\mathcal{M}_2}\right]$ para todo $1 \leq i \leq m$, $\frac{q^p - q}{n} \geq p$, $\frac{q_1^p - q_1}{m} \geq p$, onde $q = \left|\frac{R}{\mathcal{M}_1}\right|$ e $q_1 = \left|\frac{R}{\mathcal{M}_2}\right|$. Seja $g_i \in \frac{R}{\mathcal{M}_i}[X]$ um polinômio mônico, separável e irredutível com $\partial g_i = p, \ \ i = 1, 2$. Suponha que $g_1(X) = \overline{a}_o + \overline{a}_1 X + \ldots + \overline{a}_{p-1} X^{p-1} + X^p$ e $g_2(X) = \overline{b}_o + \overline{b}_1 X + \ldots + \overline{b}_{p-1} X^{p-1} + X^p$. Note que $(\overline{a_k}, \overline{b_k}) \in \frac{R}{\mathcal{M}_1} \times \frac{R}{\mathcal{M}_2}, \ \ k = 0, \ldots, p-1$. Pelo teorema do resto Chinês, existem $c_o, c_1, \ldots, c_{p-1} \in R$ tais que $\overline{c_k} = \overline{a_k}$ $(mod\ \mathcal{M}_1)$ e $\overline{c_k} = \overline{b_k}$ $(mod\ \mathcal{M}_2)$, para todo $0 \leq k \leq p-1$. Considere $f(x) = c_o + c_1 X + \ldots + c_{p-1} X^{p-1} + X^p \in R[X]$. Observe que $\overline{f} = g_1$ $(mod\ \mathcal{M}_1)$ e $\overline{f} = g_2$ $(mod\ \mathcal{M}_2)$. Então, pelo Teorema 2.2 de [14], f é um polinômio separável em $R[X]$. Mas, $\frac{S[X]}{(f)} \simeq S \otimes_R \frac{R[X]}{(f)}$ é uma S-álgebra separável. Conseqüentemente, f é separável em $S[X]$. Além disso, como ∂g_1 e $\left[\frac{S}{\mathcal{Q}_1} : \frac{R}{\mathcal{M}_1}\right]$ são coprimos, segue que g_1 é irredutível em $\frac{S}{\mathcal{Q}_1}[X]$. Portanto, f é irredutível em $S[X]$. Considere $T = \frac{S[X]}{(f)}$ e note que T/S é fortemente separável e conexa (cf. Lema 2.2.2). Denote por $N_q(n)$ o número de polinômios mônicos e irredutíveis de grau n sobre o corpo finito com q elementos. Pelo Teorema 3.25 de [18], temos $N_q(p) = \frac{q^p - q}{p} \geq n$. Logo, existem $h_1, \ldots, h_n \in \frac{R}{\mathcal{M}_1}[X]$ polinômios mônicos, separáveis e irredutíveis tais que $\partial h_j = p\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]$ para todo $1 \leq j \leq n$. De fato, se $\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right] = 1$ então $N_q\left(p\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]\right) = N_q(p) \geq n$. Se $\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right] \geq 2$ então pelo Lema 1.2 de [15] temos $N_q\left(p\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]\right) \geq N_q(p) N_q\left(\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]\right) \geq N_q(p) \geq n$. Observe que $\frac{R}{\mathcal{M}_1}$ é um corpo perfeito, pois é um corpo finito. Assim, os polinômios h_j são separáveis. Analogamente, existem $t_1, \ldots, t_m \in \frac{R}{\mathcal{M}_2}[X]$ polinômios mônicos, separáveis e irredutíveis tais que $\partial t_i = p\left[\frac{S}{\mathcal{P}_i} : \frac{R}{\mathcal{M}_2}\right]$ para todo $1 \leq i \leq m$. Pelo Teorema 3.5 de [21], T possui apenas um ideal maximal $\mathcal{Q}'_j$ sobre $\mathcal{Q}_j$ e $\left[\frac{T}{\mathcal{Q}'_j} : \frac{S}{\mathcal{Q}_j}\right] = p$. Portanto, $\left[\frac{T}{\mathcal{Q}'_j} : \frac{R}{\mathcal{M}_1}\right] = p\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]$. Desta forma, $\frac{T}{\mathcal{Q}'_j} \simeq \frac{\frac{R}{\mathcal{M}_1}[X]}{(h_j)}$ para todo $1 \leq j \leq n$.

Pelo Teorema 2.1 de [21], $\mathcal{M}T = \bigcap_{j=1}^{n} \mathcal{Q}'_j$. Usando o teorema do resto Chinês temos, $\frac{T}{\mathcal{M}_1 T} \simeq \frac{\frac{R}{\mathcal{M}_1}[X]}{(h_1 h_2 \ldots h_n)}$. Da mesma forma, pelo Teorema 3.5 de [21], T possui apenas um ideal maximal $\mathcal{P}'_i$ sobre $\mathcal{P}_i$ e $\left[\frac{T}{\mathcal{P}'_i} : \frac{R}{\mathcal{M}_2}\right] = p\left[\frac{S}{\mathcal{P}_i} : \frac{R}{\mathcal{M}_2}\right]$ para cada $1 \leq i \leq m$. Logo, $\frac{T}{\mathcal{P}'_i} \simeq \frac{\frac{R}{\mathcal{M}_2}[X]}{(t_i)}$ para todo $1 \leq i \leq m$. Novamente, pelo Teorema 2.1 de [21] e pelo teorema do resto Chinês temos $\frac{T}{\mathcal{M}_2 T} \simeq \frac{\frac{R}{\mathcal{M}_2}[X]}{(t_1 t_2 \ldots t_m)}$. Portanto, $\frac{T}{\mathcal{M}_i T}/\frac{R}{\mathcal{M}_i}$ tem elemento primitivo para $i = 1, 2$. Então, pela Proposição 2.4.2, T/R tem elemento primitivo e o resultado segue como no caso anterior.

<u>3^o caso</u>: $\left|\frac{R}{\mathcal{M}_1}\right| < \infty$ e $\left|\frac{R}{\mathcal{M}_2}\right| = \infty$.

De forma análoga ao caso anterior, considere p um número primo tal que p não divide $\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]$ para todo $1 \leq j \leq n$ e $\frac{q^p - q}{p} \geq n$, onde $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ são os ideais maximais de S que estão sobre $\mathcal{M}_1$ e $q = \left|\frac{R}{\mathcal{M}_1}\right|$. Tome $g_1 \in \frac{R}{\mathcal{M}_1}[X]$ um polinômio mônico, separável e irredutível de grau p. Como no caso anterior, existem polinômios $h_1, \ldots, h_n \in \frac{R}{\mathcal{M}_1}[X]$ mônicos, separáveis e irredutíveis tais que $\partial(h_j) = p\left[\frac{S}{\mathcal{Q}_j} : \frac{R}{\mathcal{M}_1}\right]$ para todo $1 \leq j \leq n$. Por outro lado, considere $g_2 \in \frac{R}{\mathcal{M}_2}[X]$ um polinômio mônico tal que g_2 não possui raízes repetidas no fecho algébrico de $\frac{R}{\mathcal{M}_2}$ e o grau de g_2 é p. Note que tal polinômio existe. De fato, basta tomar $x_1, \ldots, x_p \in \frac{R}{\mathcal{M}_2}$ elementos distintos e considerar $g_2(X) = (X - x_1) \ldots (X - x_p)$. De forma análoga ao caso anterior, usando o teorema do resto Chinês, obtemos um polinômio $f \in R[X]$ mônico, separável e irredutível de grau p tal que $\overline{f} = g_1 \, (mod \, \mathcal{M}_1)$ e $\overline{f} = g_2 \, (mod \, \mathcal{M}_2)$. Considerando $T = \frac{S[X]}{(f)}$, obtemos que $\frac{T}{\mathcal{M}_1 T} \simeq \frac{\frac{R}{\mathcal{M}_1}[X]}{(h_1 h_2 \ldots h_n)}$. Como $\left|\frac{R}{\mathcal{M}_2}\right| = \infty$, $\frac{T}{\mathcal{M}_2 T}/\frac{R}{\mathcal{M}_2}$ tem elemento primitivo. Assim, T/R tem elemento primitivo e o resultado segue. ■

Agora consideremos um corolário do Teorema 4.2.1.

Corolário 4.2.2. *Se R é um domínio de fatoração única (D.F.U.) semilocal então Ω_R é um domínio.*

Demonstração: Sejam $a, b \in \Omega_R$ tais que $ab = 0$. Considere uma R-subálgebra S de Ω_R a qual é uma extensão fortemente separável de R e contém a e b. Pelo Teorema 4.2.1, existe um polinômio mônico, separável e irredutível $f \in R[X]$ tal que $S \subseteq \frac{R[X]}{(f)}$. Como R é um D.F.U., temos que (f) é um ideal primo de $R[X]$. Conseqüentemente, $\frac{R[X]}{(f)}$ é um domínio. Daí, S é um domínio. Portanto, $a = 0$ ou $b = 0$. Assim, Ω_R é um domínio. ■

Observação: Sejam $L/F/K$ extensões de corpos tais que L/K é separável e $[L : K] < \infty$. Então, pelo teorema do elemento primitivo para corpos, L/K tem elemento primitivo e o número de corpos intermediários de L/K (corpos que contém K e estão contidos em L) é finito. Conseqüentemente, o número de corpos intermediários de F/K é finito e então F/K tem elemento primitivo. O Teorema 4.2.1 mostra que o mesmo não é válido no contexto de anéis comutativos. De fato, para um anel semilocal R, considere uma extensão fortemente separável e conexa S/R que não possui elemento primitivo (ver [32, pg.170]). Pelo Teorema 4.2.1, tal extensão imerge numa extensão T/R que possui elemento primitivo. Portanto, temos uma extensão fortemente separável que possui elemento primitivo com uma subálgebra intermediária que não possui elemento primitivo.

Capítulo 5

Fecho Separável

Nesse capítulo abordaremos resultados relacionados com o fecho separável de um anel conexo. Na primeira seção daremos critérios para que um polinômio separável e irredutível sobre um anel conexo R permaneça irredutível em $\frac{R}{\mathcal{M}}[X]$, para cada $\mathcal{M} \in Max(R)$. Na segunda seção relacionaremos o fecho separável de um anel conexo R com o fecho separável de certos anéis residuais obtidos via o quociente por um ideal.

5.1 Irredutibilidade

O principal resultado desta seção é o Teorema 5.1.1. Como corolário de tal resultado obtemos o Teorema 1.5 de [22].

Considere uma extensão de anéis S/R e $\mathcal{M}' \in Max(S)$. Observe que $D(\mathcal{M}') = \{\sigma \in Aut_R(S) \ : \ \sigma(\mathcal{M}') = \mathcal{M}'\}$ é um subgrupo do grupo $Aut_R(S)$. Este grupo é denominado o grupo de decomposição de $\mathcal{M}'$.

Teorema 5.1.1. *Seja R um anel conexo que satisfaz a (f.f.e.p.). As seguintes afirmações são equivalentes:*

i. A função $\Psi : Max(\Omega_R) \longrightarrow Max(R)$, dada por $\Psi(\mathcal{M}') = \mathcal{M}' \cap R$, é uma bijeção.

ii. $D(\mathcal{M}') = Aut_R(\Omega_R)$, para cada $\mathcal{M}' \in Max(\Omega_R)$.

iii. Se $f \in R[X]$ é um polinômio separável e irredutível então $\overline{f}$ é irredutível em $\frac{R}{\mathcal{M}}[X]$ para todo $\mathcal{M} \in Max(R)$.

Demonstração: $(i \to ii)$ Sejam $\mathcal{M}' \in Max(\Omega_R)$ e $\sigma \in Aut_R(\Omega_R)$ e assuma que $\mathcal{M}' \cap R = \mathcal{M}$. Então, $\sigma(\mathcal{M}') \in Max(\Omega_R)$ e $\sigma(\mathcal{M}') \cap R = \sigma(\mathcal{M}' \cap R) = \mathcal{M}$. Usando a hipótese, temos que $\sigma(\mathcal{M}') = \mathcal{M}'$. Portanto, $\sigma \in D(\mathcal{M}')$.

$(ii \to i)$ Tome $\mathcal{M}'_1, \mathcal{M}'_2 \in Max(\Omega_R)$ tais que $\mathcal{M}'_1 \cap R = \mathcal{M}$ e $\mathcal{M}'_2 \cap R = \mathcal{M}$. Pelo Lema 2.2 de [21], existe $\sigma \in Aut_R(\Omega_R)$ tal que $\sigma(\mathcal{M}'_1) = \mathcal{M}'_2$. Por hipótese, $\sigma(\mathcal{M}'_1) = \mathcal{M}'_1$. Desta forma, $\mathcal{M}'_1 = \mathcal{M}'_2$ e Ψ é uma bijeção.

$(i \to iii)$ Suponha que existem $f \in R[X]$ um polinômio separável e irredutível e $\mathcal{M} \in Max(R)$ tal que $\overline{f}$ é redutível em $\frac{R}{\mathcal{M}}[X]$. Vamos verificar que neste caso Ψ não é bijeção. Considere então $T = \frac{R[X]}{(f)}$. Pelo Teorema 3.5 de [21], T possui pelo menos dois ideais maximais sobre $\mathcal{M}$. Note que T/R é uma extensão fortemente separável. Pelo Lema 2.2.2, T é um anel conexo. Pelo Corolário 1.3.18, existe uma imersão de T em Ω_R. Daí, Ω_R possui pelo menos dois ideais maximais que estão sobre $\mathcal{M}$. Portanto, Ψ não é injetora.

$(iii \to i)$ Assuma que a função Ψ não é uma bijeção. Então, Ψ não é injetora, ou seja, existem $\mathcal{M}'_1, \mathcal{M}'_2 \in Max(\Omega_R)$ tais que $\Psi(\mathcal{M}'_1) = \Psi(\mathcal{M}'_2)$ e $\mathcal{M}'_1 \neq \mathcal{M}'_2$. Assim, $\mathcal{M}'_1 \cap R = \mathcal{M}'_2 \cap R = \mathcal{M} \in Max(R)$. Pelo Teorema 2.1 de [21], $\mathcal{M}\Omega_R = \bigcap_{\mathcal{Q} \in X} \mathcal{Q}$, onde X é o conjunto dos ideais maximais de Ω_R que estão sobre $\mathcal{M}$. Assim, $\mathcal{M}\Omega_R \subseteq \mathcal{M}'_1$. Se $\mathcal{M}\Omega_R = \mathcal{M}'_1$ então de $\mathcal{M}\Omega_R \subseteq \mathcal{M}'_1 \cap \mathcal{M}'_2 \subseteq \mathcal{M}'_1$ temos $\mathcal{M}'_1 \cap \mathcal{M}'_2 = \mathcal{M}'_1$. Portanto, $\mathcal{M}'_1 \subseteq \mathcal{M}'_2$. Da maximalidade, temos $\mathcal{M}'_1 = \mathcal{M}'_2$. Isto contradiz a escolha feita. Desta forma, $\mathcal{M}\Omega_R \subsetneq \mathcal{M}'_1$. Tome $x \in \mathcal{M}'_1 \setminus \mathcal{M}\Omega_R$. Então, existe uma extensão fortemente separável S de R, $S \subseteq \Omega_R$ tal que $x \in S$. Logo, $x \in (S \cap \mathcal{M}'_1) \setminus \mathcal{M}S$. Mas, $S \cap \mathcal{M}'_1$ é um ideal maximal de S que está sobre $\mathcal{M}$. Como $\mathcal{M}S \subsetneq S \cap \mathcal{M}'_1$, segue do Teorema 2.1 de [21], que existe um ideal maximal de S diferente de $\mathcal{M}'_1 \cap S$ que está sobre $\mathcal{M}$. Conseqüentemente, S é uma extensão fortemente separável de R que possui pelo menos dois ideais maximais que estão sobre $\mathcal{M}$. Por hipótese, existem $\alpha \in \Omega_R$ e um polinômio mônico, separável e irredutível $f(x) \in R[X]$ tal que $f(\alpha) = 0$ e $S \subseteq R[\alpha]$. Chamando $T = \frac{R[X]}{(f)}$, temos pela Proposição 2.2.3 que $T \simeq R[\alpha]$. Por hipótese, $\overline{f}(X) \in \frac{R}{\mathcal{M}}[X]$ é irredutível. Então, pelo Teorema 3.5 de [21], T possui apenas um ideal maximal que está sobre $\mathcal{M}$. Daí, $R[\alpha]$ possui apenas um ideal maximal que está sobre $\mathcal{M}$. Mas isto é uma contradição, pois $S \subseteq R[\alpha]$ é uma extensão inteira e S possui pelo menos dois ideais maximais sobre $\mathcal{M}$. ■

Observação: Note que a hipótese que R satisfaz a (f.f.e.p.) é usada apenas para demonstrar $(iii \to i)$.

Como conseqüência imediata do teorema acima e do Teorema 4.1.3 temos os seguintes corolários.

Corolário 5.1.2. *Seja R um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e localmente uniforme. As seguintes afirmações são equivalentes:*

i. A função $\Psi : Max(\Omega_R) \longrightarrow Max(R)$, dada por $\Psi(\mathcal{M}') = \mathcal{M}' \cap R$, é uma bijeção.

ii. $D(\mathcal{M}') = Aut_R(\Omega_R)$, para cada $\mathcal{M}' \in Max(\Omega_R)$.

iii. Se $f \in R[X]$ é um polinômio separável e irredutível então $\overline{f}$ é irredutível em $\frac{R}{\mathcal{M}}[X]$ para todo $\mathcal{M} \in Max(R)$.

Corolário 5.1.3. *Sejam R um anel conexo e $Max(R) = \{\mathcal{M}_1, \ldots, \mathcal{M}_t\}$. As seguintes afirmações são equivalentes:*

i. Todo polinômio separável e irredutível em $R[X]$ permanece irredutível visto em $\frac{R}{\mathcal{M}_i}[X]$ para qualquer $i = 1, \ldots, t$.

ii. $\#Max(\Omega_R) = t$.

Em [22] diz-se que um anel local $(R, \mathcal{M})$ é fracamente henseliano se cada polinômio separável e irredutível em $R[X]$ permanece irredutível em $\frac{R}{\mathcal{M}}[X]$. O próximo corolário é o Teorema 1.5 de [22] e segue imediatamente do corolário acima.

Corolário 5.1.4. *Seja $(R, \mathcal{M})$ um anel local. Então R é um anel fracamente henseliano se e somente se Ω_R é local.*

Diremos que um anel conexo R satisfaz a condição do elemento primitivo (c.e.p.) se para cada extensão fortemente separável e conexa S/R existe $\alpha \in S$ tal que $S = R[\alpha]$.

Corolário 5.1.5. *Seja R um LG-anel conexo. As seguintes afirmações são equivalentes:*

i. Todo polinômio separável e irredutível em $R[X]$ permanece irredutível em $\frac{R}{\mathcal{M}}[X]$ para qualquer $\mathcal{M} \in Max(R)$ e R satisfaz a (c.e.p.).

ii. $\Psi : Max(\Omega_R) \longrightarrow Max(R)$, dada por $\Psi(\mathcal{M}') = \mathcal{M}' \cap R$, é bijeção.

Demonstração: Assuma (i). Então, pelo teorema anterior, Ψ é bijeção. Reciprocamente, suponha que Ψ é bijeção. Pela observação feita abaixo do Teorema 5.1.1, todo polinômio separável e irredutível em $R[X]$ permanece irredutível em $\frac{R}{\mathcal{M}}[X]$ para qualquer $\mathcal{M} \in Max(R)$. Sejam S/R uma extensão fortemente separável e $\mathcal{M} \in Max(R)$. Se Ψ é bijeção então $\frac{S}{\mathcal{M}S}$ é um corpo. Pelo teorema do elemento primitivo, $\frac{S}{\mathcal{M}S}/\frac{R}{\mathcal{M}}$ tem elemento primitivo. Pela Proposição 2.4.2, S/R tem elemento primitivo. Assim, R satisfaz a c.e.p.. ■

5.2 Fecho Separável

O objetivo desta seção é generalizar dois resultados de [21]. O primeiro afirma que se $(\Omega_R, \mathcal{M}')$ é um anel local então $\Omega_{\frac{R}{\mathcal{M}}} = \frac{\Omega_R}{\mathcal{M}'}$, onde $\mathcal{M}' \in Max(\Omega_R)$ e $\mathcal{M}' \cap R = \mathcal{M}$. Provaremos que se R é um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $\mathcal{M} \in Max(R)$ então $\Omega_{\frac{R}{\mathcal{M}}} = \frac{\Omega_R}{\mathcal{M}'}$, onde $\mathcal{M}' \in Max(\Omega_R)$ e $\mathcal{M}' \cap R = \mathcal{M}$. A demonstração de tal resultado utiliza-se de argumentos via espectro booleano.

Também em [21], demonstra-se que se $(\Omega_R, \mathcal{M}')$ é um anel local e $I \subseteq R$ é um ideal então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$. Apresentamos aqui uma generalização deste resultado com a seguinte forma: se R é um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $I \subseteq J(R)$ é um ideal tal que $\frac{\Omega_R}{I\Omega_R}$ é conexo então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$.

Em seguida, apresentamos vários lemas os quais serão necessários na demonstração do próximo teorema.

Lema 5.2.1. *Sejam R um anel conexo, S/R uma extensão localmente fortemente separável e $I \subseteq R$ um ideal. Então $IS \cap R = I$.*

Demonstração: Assuma que S/R é uma extensão fortemente separável. Provaremos que, neste caso, $IS \cap R = I$. Claramente, $I \subseteq IS \cap R$. Pelo Corolário III.2.3 de [5], R é um R somando direto de S, isto é, existe um R-módulo N tal que $S = R \oplus N$. Logo, $IS = I \oplus IN$. Conseqüentemente, $IS \cap R = (I \oplus IN) \cap R$. Se $z \in (I + IN) \cap R$ então $z \in R$ e $z = x + y$ com $x \in I$ e $y \in IN$. Logo, $y = z - x \in R \cap IN \subseteq R \cap N = 0$. Portanto, $z = x \in I$. Assim, $IS \cap R = I$. Agora vamos provar o caso geral. Novamente é claro que $I \subseteq IS \cap R$. Seja $z \in IS \cap R$. Então, $z = \sum_{i=1}^{n} x_i y_i \in R$, com $x_i \in I$ e $y_i \in S$. Considere T/R uma extensão fortemente separável tal que $y_i \in T$ para cada $1 \leq i \leq n$ e $T \subseteq S$. Desta forma, $z \in IT \cap R = I$. Portanto, $IS \cap R = I$. ■

Lema 5.2.2. *Se T/R é uma extensão localmente fortemente separável e R é um anel von Neumann regular então T é um anel von Neumann regular.*

Demonstração: Seja $\alpha \in T$. Como T/R é uma extensão localmente fortemente separável, existe extensão fortemente separável S/R tal que $S \subseteq T$ e $\alpha \in S$. Se S é von Neumann regular então $\alpha = \alpha^2\beta$, para algum $\beta \in S$. Portanto, para cada elemento $\alpha \in T$ existe $\beta \in T$ tal que $\alpha = \alpha^2\beta$. Desta forma, T é von Neumann regular. Assim, é suficiente provar que uma extensão fortemente separável de um anel von Neumann regular é um anel von Neumann regular. Pelo Lema 1 de [10], S é von Neumann regular se e somente $S_{\mathcal{M}}$ é von Neumann regular para qualquer $\mathcal{M} \in Max(R)$. Mas $S_{\mathcal{M}}/R_{\mathcal{M}}$ é uma extensão fortemente separável e $R_{\mathcal{M}}$ é um corpo. Pelo teorema de Wedderburn para álgebras separáveis sobre corpos, $S_{\mathcal{M}}$ é uma soma direta finita de corpos. Logo, $S_{\mathcal{M}}$ é um anel von Neumann regular. ■

Lema 5.2.3. *Se R é um anel conexo e $I \subseteq R$ é um ideal tal que $\frac{R}{I}$ é von Neumann regular então $\frac{\Omega_R}{I\Omega_R}$ é um anel von Neumann regular.*

Demonstração: Pelo Lema 5.2.2, é suficiente provar que $\frac{\Omega_R}{I\Omega_R}/\frac{R}{I}$ é uma extensão localmente fortemente separável. Pelo Lema 5.2.1, $I\Omega_R \cap R = I$. Assim, $\frac{\Omega_R}{I\Omega_R}/\frac{R}{I}$ é uma extensão de anéis. Sejam $\alpha_1 + I\Omega_R, \alpha_2 + I\Omega_R, \ldots, \alpha_n + I\Omega_R$ elementos de $\frac{\Omega_R}{I\Omega_R}$. Então, existe S/R extensão fortemente separável tal que $\{\alpha_1, \ldots, \alpha_n\} \subseteq S \subseteq \Omega_R$. Pela Proposição 1.3.13, $\frac{S}{IS}$ é uma $\frac{R}{I}$-álgebra separável. Logo, $\frac{S}{IS}/\frac{R}{I}$ é uma extensão fortemente separável. Pela Proposição 2 de [24], Ω_R/S é uma extensão localmente fortemente separável. Pelo Lema 5.2.1, $(IS)\Omega_R \cap S = IS$. Mas $(IS)\Omega_R \cap S = I\Omega_R \cap S$. Portanto, temos uma imersão de $\frac{S}{IS}$ em $\frac{\Omega_R}{I\Omega_R}$. Identificando de maneira natural os elementos $\alpha_j + IS$ com $\alpha_j + I\Omega_R$ temos que $\frac{\Omega_R}{I\Omega_R}/\frac{R}{I}$ é uma extensão localmente fortemente separável. ■

Denote por $X(R)$ o espectro booleano de R, isto é, $X(R) = Spec(B(R)) = Max(B(R))$, onde $B(R)$ é a álgebra booleana de R.

Lema 5.2.4. *Se R é um anel von Neumann regular então $Max(R) = \{I(x) : x \in X(R)\}$.*

Demonstração: Seja $x \in X(R)$. Então, R_x é von Neumann regular e conexo. Portanto, R_x é um corpo. Mas, $R_x = \frac{R}{I(x)}$. Assim, $I(x) \in Max(R)$. Reciprocamente, dado $\mathcal{M} \in Max(R)$, considere x como sendo o conjunto dos idempotentes de R que estão em $\mathcal{M}$. É fácil verificar que x é um ideal primo de $B(R)$. Mas $Spec(B(R)) = Max(B(R))$. Desta forma, $x \in X(R)$. Mais ainda, $I(x)$ é o ideal de R gerado pelos

elementos que estão em x. Logo, $I(x) \subseteq \mathcal{M}$. Pela parte anterior, $I(x)$ é um ideal maximal de R. Ou seja, $I(x) = \mathcal{M}$. ■

Teorema 5.2.5. *Sejam R um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $\mathcal{M} \in Max(R)$. Então $\Omega_{\left(\frac{R}{\mathcal{M}}\right)} = \frac{\Omega_R}{\mathcal{M}'}$, qualquer que seja $\mathcal{M}' \in Max(\Omega_R)$ com $\mathcal{M}' \cap R = \mathcal{M}$.*

Demonstração: Seja $\mathcal{M}' \in Max(\Omega_R)$ tal que $\mathcal{M}' \cap R = \mathcal{M}$. Fixemos as seguintes notações: $\overline{R} = \frac{R}{J(R)}$ e $\overline{\Omega}_R = \frac{\Omega_R}{J(R)\Omega_R}$. Note que $J(R)\Omega_R \subseteq J(\Omega_R)$. Na verdade, pode-se verificar a igualdade, mas para nós é suficiente esta inclusão. Assim, $J(R)\Omega_R \subseteq \mathcal{M}'$ e escrevemos $\overline{\mathcal{M}'} = \frac{\mathcal{M}'}{J(R)\Omega_R}$. Vamos verificar que $\frac{\Omega_R}{\mathcal{M}'}/\frac{R}{\mathcal{M}}$ é uma extensão localmente fortemente separável. Tome $\{\alpha_1 + \mathcal{M}', \ldots, \alpha_n + \mathcal{M}'\} \subseteq \frac{\Omega_R}{\mathcal{M}'}$ um subconjunto finito. Então, existe uma extensão fortemente separável S/R tal que $S \subseteq \Omega_R$ e $\{\alpha_1, \ldots, \alpha_n\} \subseteq S$. Pela Proposição 1.3.13, $\frac{S}{\mathcal{M}S}/\frac{R}{\mathcal{M}}$ é uma extensão fortemente separável. Como Ω_R/R é uma extensão inteira, segue que $\mathcal{M}' \cap S$ é um ideal maximal de S. Pelo Teorema 2.1 de [21], $\mathcal{M}S$ é a intersecção de todos os ideais maximais de S que estão sobre $\mathcal{M}$ (ideais de S que interceptados com R são iguais a $\mathcal{M}$). Portanto, $\mathcal{M}' \cap S$ é um dos elementos desta intersecção. Pela Observação 4.1.2, o número de ideais maximais de S que estão sobre $\mathcal{M}$ é finito. Pelo teorema do resto Chinês, temos que $\frac{S}{\mathcal{M}'\cap S}$ é um somando direto de $\frac{S}{\mathcal{M}S}$. Conseqüentemente, $\frac{S}{\mathcal{M}'\cap S}/\frac{R}{\mathcal{M}}$ é uma extensão fortemente separável. Portanto, $\frac{\Omega_R}{\mathcal{M}'}/\frac{R}{\mathcal{M}}$ é uma extensão localmente fortemente separável. Falta verificar que $\frac{\Omega_R}{\mathcal{M}'}$ é separavelmente fechado. Seja $T/\frac{\Omega_R}{\mathcal{M}'}$ uma extensão fortemente separável e conexa. Pelo teorema de Wedderburn para álgebras separáveis sobre corpos temos que T é um corpo. Portanto, existe um polinômio mônico, separável e irredutível $f \in \frac{\Omega_R}{\mathcal{M}'}[X]$ tal que $T \simeq \frac{\frac{\Omega_R}{\mathcal{M}'}[X]}{(f)}$. Pelo Lema 5.2.3, $\overline{\Omega}_R$ é um anel von Neumann regular. Pelo Lema 5.2.4, existe $x \in X(\overline{\Omega}_R)$ tal que $I(x) = \overline{\mathcal{M}'}$. Portanto, $\left(\overline{\Omega}_R\right)_x = \frac{\overline{\Omega}_R}{\overline{\mathcal{M}'}} \simeq \frac{\Omega_R}{\mathcal{M}'}$. Aplicando esse isomorfismo aos coeficientes de f obtemos um polinômio mônico, separável e irredutível $u_x \in (\overline{\Omega}_R)_x[X]$. Se $u_x(X) = (a_0)_x + (a_1)_x X + \ldots + (a_{n-1})_x X^{n-1} + X^n$ então considere $u(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + X^n$. Como u_x é separável sobre $\left(\overline{\Omega}_R\right)_x$, segue do Corolário 1.3 e do Teorema 2.3 de [25] que $\delta(u_x) = \delta(u)_x$ é invertível em $\left(\overline{\Omega}_R\right)_x$. Assim, existe $\lambda \in \overline{\Omega}_R$ tal que $(\delta(u)\lambda)_x = 1_x$. Pela Proposição 1.2.8, existe uma vizinhança $N(e_1)$ de x tal que $(\delta(u)\lambda)_z = 1_z$, para qualquer $z \in N(e_1)$. Mais ainda, $(\delta(u)\lambda)e_1 = e_1$. Portanto, $u(X)e_1$ é um polinômio separável e irredutível em $\overline{\Omega}_R[X]e_1$ de grau $n = \partial(f)$. Como $N(e_1)$ é "clopen", temos que $Y = X(\overline{\Omega}_R) - N(e_1)$ é um conjunto aberto. Portanto, dado $y \in Y$ existe uma vizinhança $V_y = N(e)$

de y tal que $V_y \subseteq Y$. Tome um polinômio mônico e separável $g_y \in (\overline{\Omega}_R)_y[X]$ de grau n. Considere uma vizinhança $W_y = N(f)$ de y tal que $\delta(g)f \in U(\overline{\Omega}_R f)$. Então, $\delta(g)ef \in U(\overline{\Omega}_R ef)$. Desta forma, existe uma vizinhança $V_y \cap W_y = N(ef)$ de y tal que $N(ef) \subseteq Y$ e $g(X)ef$ é um polinômio mônico e separável em $\overline{\Omega}_R[X]ef$. Observe que para cada $y \in Y$ podemos construir o idempotente ef acima. Assim, chamaremos tal idempotente de $e(y)$. Portanto, $X(\overline{\Omega}_R) = N(e_1) \cup \left(\bigcup_{y \in Y} N(e(y)) \right)$. Note que, pela escolha das vizinhanças $N(e(y))$ temos que $N(e_1) \cap \left(\bigcup_{y \in Y} N(e(y)) \right) = \emptyset$. Usando o argumento de compacidade usual, obtemos $e_2, \ldots, e_r \in B(\overline{\Omega}_R)$ e $g_2, \ldots, g_r \in \overline{\Omega}_R[X]$ tais que $e_1 + \ldots + e_r = 1$, $e_i e_j = 0$ se $i \neq j$ e $g_i(X)e_i$ é um polinômio separável em $\overline{\Omega}_R[X]e_i$ para todo $i = 2, \ldots, r$. Tome $g = ue_1 + g_2 e_2 + \ldots + g_r e_r \in \overline{\Omega}_R[X]$. Pelo corolário 1.3 de [25], $\delta(ue_1) = \delta(u)e_1$ e $\delta(g_i e_i) = \delta(g_i)e_i$ para todo $2 \leq i \leq r$. Logo, $\delta(g) = \delta(g)e_1 + \delta(g)e_2 + \ldots + \delta(g)e_r = \delta(ge_1)e_1 + \delta(ge_2)e_2 + \ldots + \delta(ge_r)e_r = \delta(u)e_1 + \delta(g_2)e_2 + \ldots + \delta(g_r)e_r \in U(\overline{\Omega}_R)$. Assim, $g(X)$ é um polinômio mônico, separável e de grau n. Mais ainda, como $u(X)e_1$ é irredutível em $\overline{\Omega}_R[X]e_1$, temos que g é irredutível em $\overline{\Omega}_R[X]$. Seja $h \in \Omega_R[X]$ um polinômio mônico tal que $\overline{h} = g \ (mod\, J(R)\Omega_R)$. Pelo Corolário 1.3 de [25], $\overline{\delta(h)} = \delta(\overline{h}) = \delta(g) \in U(\overline{\Omega}_R)$. Conseqüentemente, $h \in R[X]$ é um polinômio separável. Ou seja, h é um polinômio mônico, separável e irredutível em $\Omega_R[X]$. Portanto, $\frac{\Omega_R[X]}{(h)}/\Omega_R$ é uma extensão fortemente separável e conexa. Logo, $\partial(h) = 1$. Desta forma, $n = 1$ e $T \simeq \frac{\Omega_R}{\mathcal{M}'}$. ■

Observe que para um anel conexo R qualquer o resultado acima não é verdadeiro. De fato, tome $R = \mathbb{Z}$ e note que $\Omega_R = R$, pois $\mathbb{Z}$ é separavelmente fechado. Tomando um ideal maximal $\mathcal{M} = p\mathbb{Z}$, onde p é um número primo temos como corpo residual o corpo finito com p elementos. Note que o fecho separável deste corpo é infinito e portanto não pode ser ele mesmo.

Em particular, se R é um anel local ou semilocal temos que $\frac{R}{J(R)}$ é von Neumann regular. O Lema 4.8 de [21], diz que se $(\Omega_R, \mathcal{M}')$ é um anel local então $\Omega_{\frac{R}{\mathcal{M}}} \simeq \frac{\Omega_R}{\mathcal{M}'}$, onde $\mathcal{M}' \cap R = \mathcal{M}$. Assim, o teorema acima generaliza este resultado.

Corolário 5.2.6. *Sejam R um conexo tal que $\frac{R}{J(R)}$ é von Neumann regular, $\mathcal{M} \in Max(R)$ e $\mathcal{M}' \in Max(\Omega_R)$ tal que $\mathcal{M}' \cap R = \mathcal{M}$. Então, $D(\mathcal{M}') = \{\sigma \in Aut_R(\Omega_R) : \sigma(\mathcal{M}') = \mathcal{M}'\} \simeq Aut_{(\frac{R}{\mathcal{M}})}\Omega_{(\frac{R}{\mathcal{M}})}$.*

Demonstração: Pelo Teorema 2.7 de [21], $D(\mathcal{M}') \simeq Aut_{\frac{R}{\mathcal{M}}} \frac{\Omega_R}{\mathcal{M}'}$. Pelo Teorema 5.2.5, $\frac{\Omega_R}{\mathcal{M}'} \simeq \Omega_{\frac{R}{\mathcal{M}}}$. Juntando as duas informações obtemos o resultado. ■

O próximo teorema generaliza o Teorema 4.9 de [21].

Teorema 5.2.7. *Sejam R um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $I \subseteq J(R)$ um ideal tal que $\frac{\Omega_R}{I\Omega_R}$ é conexo. Então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$.*

Demonstração: Conforme vimos na demonstração do Lema 5.2.3, $\frac{\Omega_R}{I\Omega_R}/\frac{R}{I}$ é uma extensão localmente fortemente separável. Agora vamos verificar que $\frac{\Omega_R}{I\Omega_R}$ é separavelmente fechado. Denote por $\overline{\Omega}_R$ o anel $\frac{\Omega_R}{I\Omega_R}$. Observe que $I\Omega_R \subseteq J(R)\Omega_R \subseteq J(\Omega_R)$. Logo, $Max(\overline{\Omega}_R) = \left\{\overline{\mathcal{M}'} = \frac{\mathcal{M}'}{I\Omega_R} \ : \ \mathcal{M}' \in Max(\Omega_R)\right\}$. Dado qualquer $\overline{\mathcal{M}'} \in Max(\overline{\Omega}_R)$, temos $\frac{\overline{\Omega}_R}{\overline{\mathcal{M}'}} \simeq \frac{\Omega_R}{\mathcal{M}'}$. Suponha que $\mathcal{M}' \cap R = \mathcal{M}$. Pelo Teorema 5.2.5, $\Omega_{\frac{R}{\mathcal{M}}} = \frac{\Omega_R}{\mathcal{M}'}$. Conseqüentemente, $\left|\frac{\Omega_R}{\mathcal{M}'}\right| = \left|\frac{\overline{\Omega}_R}{\overline{\mathcal{M}'}}\right| = \infty$. Seja $T/\overline{\Omega}_R$ uma extensão fortemente separável e conexa. Pelo Corolário 2.4.3, $\frac{T}{\overline{\mathcal{M}'}T}/\frac{\overline{\Omega}_R}{\overline{\mathcal{M}'}}$ tem elemento primitivo para qualquer $\overline{\mathcal{M}'} \in Max(\overline{\Omega}_R)$. Como R é um LG-anel e Ω_R/R é uma extensão inteira, pelo Corolário 2.3 de [8] temos que Ω_R é um LG-anel. Visto que $I\Omega_R \subseteq J(\Omega_R)$ obtemos que $\overline{\Omega}_R$ é um LG-anel. Pela Proposição 2.4.2, $T/\overline{\Omega}_R$ tem elemento primitivo. Assim, $T \simeq \frac{\overline{\Omega}_R[X]}{(f)}$, onde $f \in \overline{\Omega}_R[X]$ é um polinômio mônico, separável e irredutível. Seja $h \in \Omega_R[X]$ um polinômio mônico tal que $\overline{h} = f\,(mod\, I\Omega_R)$. Da mesma forma que na demonstração do Teorema 5.2.5, temos que $h \in \Omega_R[X]$ é um polinômio separável e irredutível. Note que, $\frac{\Omega_R[X]}{(h)}/\Omega_R$ é uma extensão fortemente separável e conexa de Ω_R. Portanto, $\partial(h) = 1$ e $T \simeq \overline{\Omega}_R$. ■

O próximo resultado é conseqüência direta do teorema acima.

Corolário 5.2.8. *Se $(R, \mathcal{M})$ é um anel local e $I \subseteq R$ é um ideal tal que $\frac{\Omega_R}{I\Omega_R}$ é conexo então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$*

Observe que se Ω_R é um anel local então R e $\frac{\Omega_R}{I\Omega_R}$ são anéis locais. Portanto, o corolário acima generaliza o Teorema 4.9 de [21].

Corolário 5.2.9. *[21, Teorema 4.9] Se Ω_R é um anel local e $I \subseteq R$ é um ideal então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$.*

Denote por $N(R)$ o nilradical de R, ou seja, $N(R)$ é o conjunto dos elementos nilpotentes de R. Pelo Lema IV.2 de [20], se R é um anel conexo e $I \subseteq N(R)$ é um ideal então $\frac{R}{I}$ é um anel conexo. Assim, temos o seguinte corolário do teorema acima.

Corolário 5.2.10. *Se R é um anel conexo tal que $\frac{R}{J(R)}$ é von Neumann regular e $I \subseteq N(R)$ é um ideal então $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$.*

Demonstração: Note que $I\Omega_R \subseteq N(R)\Omega_R \subseteq N(\Omega_R)$. Pelos comentários acima, $\frac{\Omega_R}{I\Omega_R}$ é um anel conexo. Então, pelo Teorema 5.2.7, $\Omega_{\frac{R}{I}} = \frac{\Omega_R}{I\Omega_R}$. ■

Referências Bibliográficas

[1] A. G. Aramova, *Primitive elements for cyclic p^n-extensions of commutative rings*, Math. J. Okayama Univ. **34** (1992), 13–20.

[2] M. Auslander and O. Goldman, *The brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

[3] S. Chase, D. K. Harrison, and A. Rosenberg, *Galois theory and galois cohomology of commutative rings*, Mem. Amer. Math. Soc. (1965), 15–33.

[4] F. DeMeyer, *Separable polynomials over a commutative ring*, Rocky Mountain J. Math. **2** (1972), 299–310.

[5] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lectures Notes in Mathematics, Springer-Verlag, New-York, 1970.

[6] C. Dragos, *On normal polynomials and polynomials which generate the same extension*, Journal of Number Theory **34** (1990), 271–275.

[7] O. Endler, *Valuation theory*, Springer-Verlag, New York, 1972.

[8] D. R. Estes and R. M. Guralnick, *Module equivalences:local to global when primitive polynomials represent units*, Journal of Algebra **77** (1982), 138–157.

[9] M. Ferrero and A. Paques, *Galois theory of commutative rings revisited*, Contributions to Algebra and Geometry **38** (1997), 399–410.

[10] K. R. Goodearl and R. B. Warfield, *Algebras over zero-dimensional rings*, Math. Ann. **223** (1976), 157–168.

[11] D. K. Harrison and T. McKenzie, *Toward an arithmetic of polynomials*, Aequationes Mathematicae **43** (1992), 21–37.

[12] H. Hasse, *Zwei existenszsätze über algebraische zahlkörper*, Math. Ann. **95** (1925), 229–238.

[13] E. C. Ingraham, *Inertial subalgebras of algebras over commutative rings*, Trans. Amer. Math. Soc. **124** (1966), 77–93.

[14] G. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479.

[15] I. Kikumasa, *On primitive elements of galois extensions of commutative semilocal rings ii*, Math. J. Okayama Univ. **31** (1989), 57–71.

[16] I. Kikumasa and T. Nagahara, *Primitive elements of cyclic extensions of commutative rings*, Math. J. Okayama Univ. **29** (1987), 91–102.

[17] I. Kikumasa, T. Nagahara, and K. Kishimoto, *On primitive elements of galois extensions of commutative semilocal rings*, Math. J. Okayama Univ. **31** (1989), 31–55.

[18] R. Lidl and Niederreiter, *Finite fields*, Addison-Wesley, 1983.

[19] A. R. Magid, *The separable galois theory of commutative rings*, Pure and Applied Mathematics, Marcel Dekker, 1974.

[20] B. McDonald, *Linear algebra over commutative rings*, Marcel Dekker, 1984.

[21] T. McKenzie, *Separable polynomials and weak henselizations*, Lectures Notes in Pure and Appl. Math. **159** (1994), 165–179.

[22] ———, *Weakly henselian rings*, Math. J. Okayama Univ. **38** (1996), 47–51.

[23] ———, *The separable closure of a local ring*, J. of Algebra **207** (1998), 657–663.

[24] T. Nagahara, *On separable extensions of domains*, Math. J. Okayama Univ. **14** (1970), 145–151.

[25] ———, *On separable polynomials over a commutative ring ii*, Math. J. Okayama Univ. **15** (1972), 149–162.

[26] A. Paques, *On the primitive element and normal basis theorems*, Communications in Algebra **16** (1988), no. 3, 443–455.

[27] J-D. Thérond, *Le théorème de l'élément primitif pour un anneau semi-local*, Journal of Algebra **105** (1987), 29–39.

[28] O. E. Villamayor, *Separable algebras and galois extensions*, Osaka J. Math. **4** (1967), 161–171.

[29] O. E. Villamayor and D. Zelinsky, *Galois theory with finitely many idempotents*, Nagoya Math. J. **27** (1966), 721–731.

[30] ———, *Galois theory with infinitely many idempotents*, Nagoya Math. J. **35** (1969), 83–98.

[31] William C. Waterhouse, *The normal basis theorem*, Amer.Math.Monthly **86** (1979), no. 3, 212.

[32] E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.